

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-255431

(43)Date of publication of application : 19.09.2000

(51)Int.Cl. B61L 23/04
G05B 9/03

(21)Application number : 11-055774 (71)Applicant : EAST JAPAN RAILWAY CO
TOSHIBA CORP

(22)Date of filing : 03.03.1999 (72)Inventor : ICHIKAWA NORIAKI
MEGURO TAKAYUKI
OTANI YOSHIYUKI
ISONO KYOSUKE
NAGASHIMA TERUZO
YASUMOTO TAKANORI

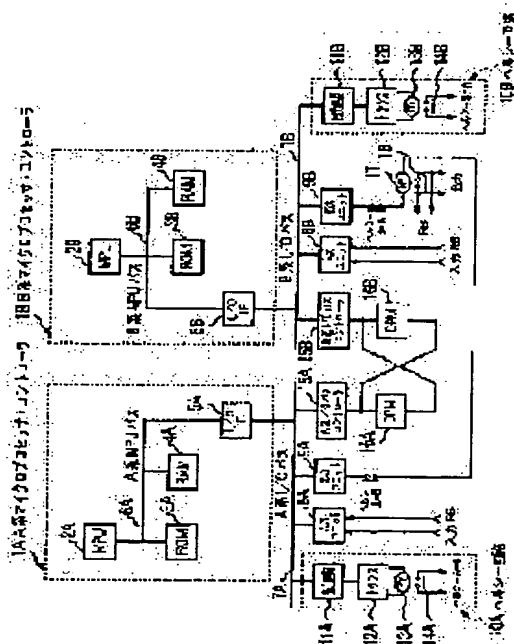
(54) SAFETY CONTROL DEVICE FOR AND SAFETY CONTROL SYSTEM OF RAILWAY

(57)Abstract:

PROBLEM TO BE SOLVED: To enhance fail safe with a simple configuration.

SOLUTION: Input units 8A, 8B apply input signals from on-site devices to controllers 1A, 1B, respectively. The controllers 1A, 1B carry out operation based on the inputs of the signals to apply control signals to the on-site devices via output units 9A, 9B. In carrying out an input process, an operation process, and an input process, the controllers 1A, 1B carry out the collation of a self system and a mating system through common memories 16A, 16B. Disagreed data finds a fault to stop running. Healthy circuits 10A, 10B are circuits for applying signals indicating that the self system is in health.

Applying signals indicating that any one of the systems is in abnormal applies no signals from the output units 9A, 9B.



LEGAL STATUS

[Date of request for examination] 05.09.2002

[Date of sending the examiner's decision
of rejection]

BEST AVAILABLE COPY

[Kind of final disposal of application
other than the examiner's decision of
rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-255431

(P2000-255431A)

(43) 公開日 平成12年9月19日 (2000.9.19)

(51) Int.Cl.⁷

識別記号

F I

ターコード (参考)

B 6 1 L 23/04

B 6 1 L 23/04

5 H 2 0 9

G 0 5 B 9/03

G 0 5 B 9/03

審査請求 未請求 請求項の数15 O L (全 22 頁)

(21) 出願番号 特願平11-55774

(22) 出願日 平成11年3月3日 (1999.3.3)

(71) 出願人 000221616

東日本旅客鉄道株式会社

東京都渋谷区代々木二丁目二番二号

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 市川 憲 照

東京都渋谷区代々木二丁目2番2号 東日

本旅客鉄道株式会社内

(74) 代理人 100064285

弁理士 佐藤 一雄 (外3名)

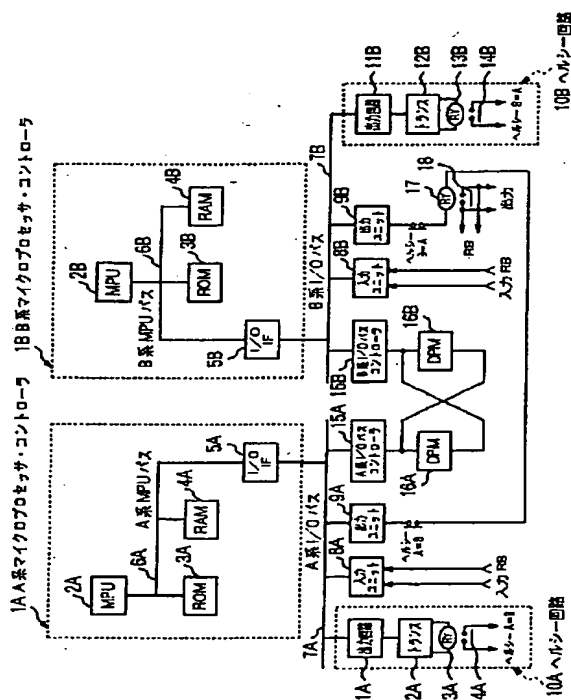
最終頁に続く

(54) 【発明の名称】 鉄道用保安制御装置及び保安制御システム

(57) 【要約】

【課題】 簡単な構成によって、フェイルセーフ性を向上させること。

【解決手段】 入力ユニット8A、8Bは、それぞれ現場機器からの入力信号をコントローラ1A、1Bに出力する。コントローラ1A、1Bはこの信号の入力に基づき演算を行い制御信号を出力ユニット9A、9Bを介して現場機器に出力する。コントローラ1A、1Bは、入力処理、演算処理、及び出力処理を行うに際して、共有メモリ16A、16Bを通して互いに自系と他系との照合を行い、データが一致しない場合は故障であるとして走行を停止する。ヘルシー回路10A、10Bは自系が健全であることを示す信号を出力する回路であり、一方が異常を示す信号を出力すると出力ユニット9A、9Bから信号が出力されない。



(2)

【特許請求の範囲】

【請求項1】現場機器に対する制御が可能少なくとも2系統以上の制御系を有し、この2系統以上の制御系はそれぞれに専用のマイクロプロセッサ・コントローラを有している鉄道用保安制御装置において、

前記各制御系は、

自系統側及び1つの他系統側の入出力結果を記憶し、前記現場機器との間の信号の入出力結果について、自系統側と1つの他系統側との間で一致するか否かを照合するための共有メモリと、自系統側又は照合相手の他系統側が正常状態又は故障状態のいずれにあるかを示す信号を出力するヘルシー回路と、を有しており、

各制御系の前記マイクロプロセッサ・コントローラは、前記共有メモリを用いて前記照合を行い、その照合結果の組合せが所定の場合にのみ前記現場機器に対する制御を実行すると共に、自系統側又は1つの他系統側のいずれかのヘルシー回路から故障状態を示す信号を入力した場合は、その制御動作を停止するものであり、

前記ヘルシー回路は、交番信号を出力する交番信号出力回路と、前記交番信号出力回路からの交番信号を1次側に入力し2次側から交番信号の交流分のみを出力するトランスと、前記トランスからの交番信号を整流した入力により動作するヘルシーリレー接点と、を有するものである、

ことを特徴とする鉄道用保安制御装置。

【請求項2】前記各制御系は、前記現場機器からの信号を入力する専用の入力ユニットを有するものであり、さらに、各制御系のマイクロプロセッサ・コントローラは、それぞれ自系統側の故障を診断する機能を備えると共に、1つの他系統側の故障診断結果との照合を行う機能を備えており、

自系統側の入力ユニットの入力信号と1つの他系統側の入力ユニットの入力信号とが一致しない場合は、双方の制御系の制御動作を停止し、前記両機能に基づいて危険側故障を確実に検出するようにした、

ことを特徴とする請求項1記載の鉄道用保安制御装置。

【請求項3】前記各制御系の入力ユニットは、前記現場機器からの信号入力経路上に設けられた入力用半導体素子と、この入力用半導体素子に直列接続されたチェック用半導体素子とを有しており、

前記各制御系のマイクロプロセッサ・コントローラは、前記入力用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を行うチェック信号発生回路を有するものである、

ことを特徴とする請求項2記載の鉄道用保安制御装置。

【請求項4】前記各制御系は、前記現場機器に対する出力信号を出力し、且つその信号出力経路が互いに直列接続されている専用の出力ユニットを有するものであり、自系統側の出力ユニットの出力信号と1つの他系統側の出力ユニットの出力信号とが一致しない場合は、双方の

制御系の制御動作を停止するようにした、

ことを特徴とする請求項1乃至3のいずれかに記載の鉄道用保安制御装置。

【請求項5】前記各出力ユニットは、それぞれ前記信号出力経路上に設けられた出力用半導体素子と、この出力用半導体素子のオンオフ状態とは反対のオンオフ状態を示す故障検出用半導体素子と、この故障検出用半導体素子に流れる電流を定期的にオンオフさせてこの故障検出用半導体素子自体の故障の有無をチェックするチェック用半導体素子と、を有しており、

前記各マイクロプロセッサ・コントローラは、前記出力用半導体素子をオンオフさせる出力信号駆動回路と、前記故障検出用半導体素子のオンオフ状態の検出により前記出力用半導体素子についての故障の有無を検出する故障検出回路と、前記故障検出用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を定期的に行うチェック信号発生回路と、前記現場機器のリレー接点状態を読み取る接点リードバック回路と、を有しており、これら各回路の入力状態又は出力状態に基づいて、前記各出力ユニットについての故障状態を判別するものである、

ことを特徴とする請求項4記載の鉄道用保安制御装置。

【請求項6】前記各マイクロプロセッサ・コントローラは、前記自系統側の出力ユニットの出力用半導体素子又は前記1つの他系統側の出力ユニットの出力用半導体素子のいずれか一方が半導通状態にあることを検出可能なものである、

ことを特徴とする請求項5記載の鉄道用保安制御装置。

【請求項7】前記各制御系のマイクロプロセッサ・コントローラは、メインプログラムを実行する制御処理手段と、前記メインプログラムに所定時間毎に割り込みプログラムの割り込みをかけて前記交番信号を発生させる交番信号発生手段とを有し、

前記制御処理手段及び前記交番信号発生手段は、前記メインプログラムの1回の処理時間における割込プログラムの割込回数をそれぞれ監視し、この割込回数の値が所定範囲外となった場合に、マイクロプロセッサ・コントローラの制御を停止させるものである、

ことを特徴とする請求項1記載の鉄道用保安制御装置。

【請求項8】前記共有メモリは、前記自系統側又は前記1つの他系統側のマイクロプロセッサ・コントローラのうちのいずれかのプログラム内容の一部が書き換えられた場合に、その書き換えられた内容を記憶可能なものであり、

前記自系統側又は前記1つの他系統側のマイクロプロセッサ・コントローラのうちのいずれか一方のプログラム内容の一部が書き換えられた場合には、他方のプログラム内容も同様に書き換えられるようになっている、

ことを特徴とする請求項1乃至7のいずれかに記載の鉄道用保安制御装置。

(3)

【請求項9】前記制御系のいずれかに故障が発生した場合、その制御系のマイクロプロセッサ・コントローラを他の制御系から強制的に切断するため、このコントローラの電源回路をオフにすることによりこのコントローラの動作を停止させる、
ことを特徴とする請求項1乃至8のいずれかに記載の鉄道用保安制御装置。

【請求項10】前記制御系が第1乃至第3の3つの制御系により構成され、いずれか1つの制御系に故障が発生した場合に、残りの2つの制御系に故障が発生していないことを前記照合機能を用いて検出したときのみ、この残りの2つの制御系により前記現場機器に対する制御を継続する、
ことを特徴とする請求項1記載の鉄道用保安制御装置。

【請求項11】前記第1乃至第3の3つの制御系の全てによる制御動作実行中に、いずれか2つの制御系が残りの制御系の故障を検出した場合は、残りの1つの制御系のマイクロプロセッサ・コントローラの電源回路がオフとなり、

また、前記第1乃至第3の3つの制御系のうちのいずれか2つの制御系による制御動作実行中に、一方の制御系が他方の制御系の故障を検出した場合は、双方の制御系のマイクロプロセッサ・コントローラの電源回路がオフとなる、
ことを特徴とする請求項10記載の鉄道用保安制御装置。

【請求項12】前記各制御系のマイクロプロセッサ・コントローラは、タイマのカウント値に基づきメインプログラムにおける所定動作実行時点を決定し、この時点で前記自系統側と1つの他系統側との間の照合を行う場合に、この時点から所定時間が経過するまでの期間における照合結果を無効とすることにより、前記自系統側のタイマと1つの他系統側のタイマとの間のカウントタイミングのずれに起因する照合エラーを排除するようにした、

ことを特徴とする請求項1乃至11のいずれかに記載の鉄道用保安制御装置。

【請求項13】現場機器との間で信号の授受を行う複数の入出力端末装置と少なくとも1台の制御処理端末装置との間を通信ネットワークで接続し、この制御処理端末装置がこれら複数の入出力端末装置を介して複数の現場機器に対する制御を行う制御システムにおいて、前記入出力端末装置及び前記制御処理端末装置を、前記請求項1乃至12のいずれかに記載の鉄道用保安制御装置により構成した、

ことを特徴とする鉄道用保安制御システム。

【請求項14】前記制御処理端末装置は、現在の列車運行用の第1の制御処理端末装置と、新しい応用プログラムが実装された第2の制御処理端末装置とで構成され、列車運行数が多い時間帯では、第1の制御処理端末装置

が全ての入出力端末装置との間で信号の授受を行い、列車運行数が少ない時間帯では、第1の制御処理端末装置は特定の入出力端末装置との間でのみ信号の授受を行うと共に、第2の制御処理端末装置は残りの入出力端末装置との間で信号の授受を行う、

ことを特徴とする請求項13記載の鉄道用保安制御システム。

【請求項15】前記各入出力端末装置は、前記第1の制御処理端末装置又は前記第2の制御処理端末装置のうちのいずれと信号の授受を行うかを定める切換スイッチを有しており、この切換スイッチの制御は前記第2の制御処理端末装置により行われるようになっている、
ことを特徴とする請求項14記載の鉄道用保安制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、鉄道用保安制御装置及び保安制御システムに関するものである。

【0002】

【従来の技術】一般に、鉄道用列車の制御装置に対しては、万一故障が発生したとしても、その装置は常に安全側の状態となるようにして、危険側の状態になるのを回避できるような機能が要求されており、このような機能をフェイルセーフ機能と呼んでいる。例えば、信号制御装置においては、安全側の故障状態とは、列車の進行を許可する信号（青信号）を出力すべきであるにもかかわらず、列車の進行を禁止する信号（赤信号）が誤って出力されているような状態であり、一方、危険側の故障状態とは、列車の進行を禁止する信号（赤信号）を出力すべきであるにもかかわらず、列車の進行を許可する信号（青信号）が誤って出力されているような状態である。また、踏切制御装置においては、安全側の故障状態とは、遮断機を上げる信号を出力すべきであるにもかかわらず、遮断機を下ろす信号が誤って出力されているような状態であり、一方、危険側の故障状態とは、遮断機を下げる信号を出力すべきであるにもかかわらず、遮断機を上げる信号が誤って出力されているような状態である。

【0003】図19は、このようなフェイルセーフ機能が要求されている従来の鉄道用保安制御装置の要部の構成を示すブロック図である。この制御装置は、A系及びB系から成る2重系の構成を有しており、A系及びB系はそれぞれマイクロプロセッサ・ユニット101A、101B及びメモリ102A、102Bを有している。これらマイクロプロセッサ・ユニット101A、101Bはクロック回路103からのクロック信号により同期を取りながら走行している。

【0004】マイクロプロセッサ・ユニット101A、101Bにはバス104A、104Bを介してバス照合・交番信号出力回路105が接続されている。このバス

(4)

照合・交番信号出力回路105は、バス104A、104B上に現れるマイクロプロセッサ・ユニット101A、104Bの信号を照合し、両者が一致するか否かについてその照合結果を照合異常検出回路106に出力している。バス照合・交番信号出力回路105は、常時、交番信号を出力しており、両者が一致している場合は、この交番信号の出力を継続することによりマイクロプロセッサ・ユニット101A、101Bの走行を許容する。

【0005】しかし、バス照合・交番信号出力回路105は、両者の信号の不一致が一度でも発生すると、この不一致の情報を記憶し、以後の交番信号の出力を停止する。バス照合・交番信号出力回路105からの交番信号の停止で、照合異常検出回路106は照合異常を検出し、マイクロプロセッサ・ユニット101A、101Bにリセット信号を出力する。マイクロプロセッサ・ユニット101A、101Bがリセットされることにより、バス照合・交番信号出力回路105が照合すべきデータがなくなり、照合不一致となって交番信号を出力できなくなる。

【0006】そして、双方のマイクロプロセッサ・ユニット101A、101Bはリセットされた状態（安全側の状態となっている）で走行を停止するので、上記のフェイルセーフ機能が確保されることになる。

【0007】

【発明が解決しようとする課題】従来の鉄道用保安制御装置は、上記したように、図19のような構成のフェイルセーフ回路によってフェイルセーフ機能が確保されている。しかし、図19に示したフェイルセーフ回路は、通常、専用のハードウェアにより構成されている。したがって、高性能のマイクロプロセッサ・ユニットやマイクロコンピュータが開発される度に、その都度専用のハードウェアを開発しなければならず、多大の労力及びコストを費やす結果となっていた。

【0008】また、最近の鉄道用保安制御装置には多くの個所に半導体素子が使用されているが、これらの半導体素子の故障の発生場所あるいは発生状態によってはフェイルセーフ機能を確保できない場合も考えられ、フェイルセーフ性を一定以上向上させることが非常に困難であった。

【0009】本発明は、上記事情に鑑みてなされたものであり、簡単な構成によって、フェイルセーフ性を向上させることが可能な鉄道用保安制御装置及び保安制御システムを提供することを目的としている。

【0010】

【課題を解決するための手段】上記課題を解決するための手段として、請求項1記載の発明は、現場機器に対する制御が可能な少なくとも2系統以上の制御系を有し、この2系統以上の制御系はそれぞれに専用のマイクロプロセッサ・コントローラを有している鉄道用保安制御装

置において、前記各制御系は、自系統側及び1つの他系統側の入出力結果を記憶し、前記現場機器との間の信号の入出力結果について、自系統側と1つの他系統側との間で一致するか否かを照合するための共有メモリと、自系統側又は照相手側の他系統側が正常状態又は故障状態のいずれにあるかを示す信号を出力するヘルシー回路と、を有しており、各制御系の前記マイクロプロセッサ・コントローラは、前記共有メモリを用いて前記照合を行い、その照合結果の組合せが所定の場合にのみ前記現場機器に対する制御を実行すると共に、自系統側又は1つの他系統側のいずれかのヘルシー回路から故障状態を示す信号を入力した場合は、その制御動作を停止するものであり、前記ヘルシー回路は、交番信号を出力する交番信号出力回路と、前記交番信号出力回路からの交番信号を1次側に入力し2次側から交番信号の交流分のみを出力するトランスと、前記トランスからの交番信号を整流した入力により動作するヘルシーリレー接点と、を有するものである、ことを特徴とする。

【0011】請求項2記載の発明は、請求項1記載の発明において、前記各制御系は、前記現場機器からの信号を入力する専用の入力ユニットを有するものであり、さらに、各制御系のマイクロプロセッサ・コントローラは、それぞれ自系統側の故障を診断する機能を備えると共に、1つの他系統側の故障診断結果との照合を行う機能を備えており、自系統側の入力ユニットの入力信号と1つの他系統側の入力ユニットの入力信号とが一致しない場合は、双方の制御系の制御動作を停止し、前記両機能に基づいて危険側故障を確実に検出するようにした、ことを特徴とする。

【0012】請求項3記載の発明は、請求項2記載の発明において、前記各制御系の入力ユニットは、前記現場機器からの信号入力経路上に設けられた入力用半導体素子と、この入力用半導体素子に直列接続されたチェック用半導体素子とを有しており、前記各制御系のマイクロプロセッサ・コントローラは、前記入力用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を行うチェック信号発生回路を有するものである、ことを特徴とする。

【0013】請求項4記載の発明は、請求項1乃至3のいずれかに記載の発明において、前記各制御系は、前記現場機器に対する出力信号を出力し、且つその信号出力経路が互いに直列接続されている専用の出力ユニットを有するものであり、自系統側の出力ユニットの出力信号と1つの他系統側の出力ユニットの出力信号とが一致しない場合は、双方の制御系の制御動作を停止するようにした、ことを特徴とする。

【0014】請求項5記載の発明は、請求項4記載の発明において、前記各出力ユニットは、それぞれ前記信号出力経路上に設けられた出力用半導体素子と、この出力用半導体素子のオンオフ状態とは反対のオンオフ状態を

(5)

示す故障検出用半導体素子と、この故障検出用半導体素子に流れる電流を定期的にオンオフさせてこの故障検出用半導体素子自体の故障の有無をチェックするチェック用半導体素子と、を有しており、前記各マイクロプロセッサ・コントローラは、前記出力用半導体素子をオンオフさせる出力信号駆動回路と、前記故障検出用半導体素子のオンオフ状態の検出により前記出力用半導体素子についての故障の有無を検出する故障検出回路と、前記故障検出用半導体素子の導通故障又はオープン故障を検出するために、チェック信号の出力又はその出力停止を定期的に行うチェック信号発生回路と、前記現場機器のリレー接点状態を読み取る接点リードバック回路と、を有しており、これら各回路の入力状態又は出力状態に基づいて、前記各出力ユニットについての故障状態を判別するものである、ことを特徴とする。

【0015】請求項6記載の発明は、請求項5記載の発明において、前記各マイクロプロセッサ・コントローラは、前記自系統側の出力ユニットの出力用半導体素子又は前記1つの他系統側の出力ユニットの出力用半導体素子のいずれか一方が半導通状態にあることを検出可能なものである、ことを特徴とする。

【0016】請求項7記載の発明は、請求項1記載の発明において、前記各制御系のマイクロプロセッサ・コントローラは、メインプログラムを実行する制御処理手段と、前記メインプログラムに所定時間毎に割り込みプログラムの割り込みをかけて前記交番信号を発生させる交番信号発生手段とを有し、前記制御処理手段及び前記交番信号発生手段は、前記メインプログラムの1回の処理時間における割り込みプログラムの割り込み回数をそれぞれ監視し、この割り込み回数の値が所定範囲外となった場合に、マイクロプロセッサ・コントローラの制御を停止させるものである、ことを特徴とする。

【0017】請求項8記載の発明は、請求項1乃至7のいずれかに記載の発明において、前記共有メモリは、前記自系統側又は前記1つの他系統側のマイクロプロセッサ・コントローラのうちのいずれかのプログラム内容の一部が書き換えられた場合に、その書き換えられた内容を記憶可能なものであり、前記自系統側又は前記1つの他系統側のマイクロプロセッサ・コントローラのうちのいずれか一方のプログラム内容の一部が書き換えられた場合には、他方のプログラム内容も同様に書き換えられるようになっている、ことを特徴とする。

【0018】請求項9記載の発明は、請求項1乃至8のいずれかに記載の発明において、前記制御系のいずれかに故障が発生した場合、その制御系のマイクロプロセッサ・コントローラを他の制御系から強制的に切断するため、このコントローラの電源回路をオフにすることによりこのコントローラの動作を停止させる、ことを特徴とする。

【0019】請求項10記載の発明は、請求項1記載の

発明において、前記制御系が第1乃至第3の3つの制御系により構成され、いずれか1つの制御系に故障が発生した場合に、残りの2つの制御系に故障が発生していないことを前記照合機能を用いて検出したときのみ、この残りの2つの制御系により前記現場機器に対する制御を継続する、ことを特徴とする。

【0020】請求項11記載の発明は、請求項10記載の発明において、前記第1乃至第3の3つの制御系の全てによる制御動作実行中に、いずれか2つの制御系が残りの制御系の故障を検出した場合は、残りの1つの制御系のマイクロプロセッサ・コントローラの電源回路がオフとなり、また、前記第1乃至第3の3つの制御系のうちのいずれか2つの制御系による制御動作実行中に、一方の制御系が他方の制御系の故障を検出した場合は、双方の制御系のマイクロプロセッサ・コントローラの電源回路がオフとなる、ことを特徴とする。

【0021】請求項12記載の発明は、請求項1乃至11のいずれかに記載の発明において、前記各制御系のマイクロプロセッサ・コントローラは、タイマのカウント値に基づきメインプログラムにおける所定動作実行時点を決定し、この時点で前記自系統側と1つの他系統側との間の照合を行う場合に、この時点から所定時間が経過するまでの期間における照合結果を無効とすることにより、前記自系統側のタイマと1つの他系統側のタイマとの間のカウントタイミングのずれに起因する照合エラーを排除するようにした、ことを特徴とする。

【0022】請求項13記載の発明は、現場機器との間で信号の授受を行う複数の入出力端末装置と少なくとも1台の制御処理端末装置との間を通信ネットワークで接続し、この制御処理端末装置がこれら複数の入出力端末装置を介して複数の現場機器に対する制御を行う制御システムにおいて、前記入出力端末装置及び前記制御処理端末装置を、前記請求項1乃至12のいずれかに記載の鉄道用保安制御装置により構成した、ことを特徴とする。

【0023】請求項14記載の発明は、請求項13記載の発明において、前記制御処理端末装置は、現在の列車運行用の第1の制御処理端末装置と、新しい応用プログラムが実装された第2の制御処理端末装置とで構成され、列車運行数が多い時間帯では、第1の制御処理端末装置が全ての入出力端末装置との間で信号の授受を行い、列車運行数が少ない時間帯では、第1の制御処理端末装置は特定の入出力端末装置との間でのみ信号の授受を行うと共に、第2の制御処理端末装置は残りの入出力端末装置との間で信号の授受を行う、ことを特徴とする。

【0024】請求項15記載の発明は、請求項14記載の発明において、前記各入出力端末装置は、前記第1の制御処理端末装置又は前記第2の制御処理端末装置のうちのいずれと信号の授受を行うかを定める切換スイッチ

(6)

を有しており、この切換スイッチの制御は前記第2の制御処理端末装置により行われるようになっている、ことを特徴とする。

【0025】

【発明の実施の形態】以下、本発明の実施形態を図に基づき説明する。但し、以下の実施形態では、鉄道用保安制御装置及び鉄道用保安制御システムとして、電子踏切制御装置及び電子踏切制御システムを例にとり説明するが、本発明の技術の適用はこれらのみに限定されるわけではなく、信号制御装置及び信号制御システムなどの他の制御装置及び制御システムに適用可能なものである。

【0026】図1は第1の実施形態の構成を示すブロック図である。この第1の実施形態は、A系（第1の制御系）及びB系（第2の制御系）の2つの制御系を有するものである。

【0027】図1において、まず、A系の構成を説明すると、A系マイクロプロセッサ・コントローラ1Aはマイクロプロセッサ・ユニット2A、ROMにより構成された記憶部3A、RAMにより構成された記憶部4A、入出力インタフェイス5Aを有しており、これらはMPUバス6Aにより相互に接続されている。

【0028】入出力インタフェイス5AはI/Oバス7Aに接続されており、このI/Oバス7Aには、また、入力ユニット8A、出力ユニット9A、及びヘルシー回路10Aも接続されている。このヘルシー回路10Aは、出力回路11A、トランス12A、リレー13A、及びヘルシーリレー接点14A等により構成されている。I/Oバス7AはI/Oバスコントローラ15Aにより制御されるようになっており、このI/Oバスコントローラ15Aに共有メモリ16Aが接続されている。

【0029】B系の構成もA系と同様であるため、B系についてはその重複した説明を省略する。出力ユニット9A、9B間には現場機器のリレー17が接続されており、そのリレー接点18のオンオフにより、例えば遮断機の制御が行われるようになっている。そして、リレー接点18の状態は、リードバック（RB）信号として入力ユニット8A、8Bに入力されるようになっている。

【0030】マイクロプロセッサ・ユニット2Aは、データの入出力制御、各種演算、シリアルデータ伝送等を行うものである。記憶部3Aは、マイクロプロセッサ・ユニット2Aのプログラムを格納するものであり、この実施形態では電氣的な書込・消去が可能なEEPROMにより形成されている。記憶部4Aは、ユーザアプリケーション・プログラムとマイクロプロセッサ・ユニット2Aの動作に必要なメモリである。入出力インタフェイス5Aは、MPUバス6AとI/Oバス7Aとの間のインタフェイスを行うものであり、ゲートアレイにより構成されている。

【0031】入力ユニット8Aは、例えば所定区間における列車の存在を知らせる信号、あるいは上述したリ

ードバック信号等を入力し、これをA系マイクロプロセッサ・コントローラ1Aに送出するものである。

【0032】出力ユニット9Aは、A系マイクロプロセッサ・コントローラ1Aからの制御信号を出力し、リレー17の制御を行うものである。但し、後述するように、このリレー17は、出力ユニット9A、9Bの出力値が動作方向で一致した場合のみ動作するようになっている。

【0033】共有メモリ16A、16Bには、それぞれ自系の入力データや出力データ等が記憶されるようになっている。しかし、I/Oバスコントローラ15A、15Bの制御により、コントローラ1A、1Bはそれぞれ自系の共有メモリの内容だけでなく、他系の共有メモリの内容についても読み取ることができるようになっている。

【0034】ヘルシー回路10Aは、自系が正常な状態であるか否かを示す信号を出力する回路である。正常な状態の場合は、出力回路11Aからの交番信号がトランス12Aを介してリレー13Aを励磁し、ヘルシーリレー接点14Aがオン状態となる。一方、故障状態の場合は、ヘルシーリレー接点14Aはオフとなる。ヘルシーリレー接点14Aがオフとなっている場合は、もちろんA系は制御を停止しているが、ヘルシーリレー接点14Aがオフになるとヘルシーリレー接点14Bもオフとなり、B系も結局制御を停止するようになっている。

【0035】上記した図1の構成は、コントローラ部分が他の部分とI/Oインタフェイスで分離されており、独立性が強いものとなっている。したがって、汎用性の高いボードコンピュータ等を採用することができ、マイクロプロセッサのみを高機能の機種と交換することによって、機能の向上や新機種への対応を容易に図ることが可能な構成となっている。

【0036】図2は、図1における入力ユニット8A、8Bの構成と、この入力ユニット8A、8Bとの間で信号の授受を行うマイクロプロセッサ・コントローラ1A、1Bの構成とを示すブロック図である。この図において、入力ユニット8Aは、抵抗19Aと、発光ダイオード21A及びフォトトランジスタ22Aにより形成されるフォトカプラ20A（入力用半導体素子）と、発光ダイオード24A及びフォトトランジスタ25Aにより形成されるフォトカプラ23A（チェック用半導体素子）とを有している。

【0037】コントローラ1Aは、故障診断回路26Aと、信号入力回路27Aと、比較照合回路28Aと、チェック信号発生回路29Aとを有している。そして、入力ユニット8B及びコントローラ1Bも入力ユニット8A及びコントローラ1Aと同様の構成を有している。

【0038】入力ユニット8A、8Bには入力接点信号S1が入力されるようになっている。入力接点信号S1は、踏切付近の所定区間内に列車が存在するか否かを知

(7)

らせる2値信号であり、“0”は列車が存在する場合、“1”は列車が存在しない場合を示している。ここで、入力ユニット8A、8Bのフェイルセーフ機能について説明すると、信号S1の入力の際のフェイルセーフ性とは、信号“0”を誤って信号“1”と判別してしまうことを確実に防止することをいう。

【0039】すなわち、入力ユニットに何らかの故障が生じ、実際の入力信号“0”（列車が存在する）を入力信号“1”（列車が存在しない）と誤って認識して遮断機を開放した場合には重大事故に直結する虞れがあるので、このような故障は絶対に回避しなければならない。このような故障を「危険側故障」と呼ぶ。これに対し、実際の入力信号“1”（列車が存在しない）を入力信号“0”（列車が存在する）と誤って認識させるような故障は直ちに重大事故に直結するものではないため、このような故障を「安全側故障」と呼ぶ。図2の構成は、上記の危険側故障に起因する事故を確実に防止するためのものである。

【0040】次に、図2の動作につき説明する。まず、入力ユニット8A、8Bのいずれにも故障が生じていない場合を考える。例えば、入力接点信号S1として信号“0”が入力ユニット8A、8Bに入力されると、入力ユニット8A内の抵抗19A、発光ダイオード21A、フォトトランジスタ25Aの経路には電流が流れないので、コントローラ1A内の信号入力回路27Aも“0”を入力する。この入力結果は共有メモリ16に書き込まれる。入力ユニット8B及びコントローラ1B内でも同様の動作が行われる。

【0041】比較照合回路28Aは、共有メモリ16に書き込まれている信号入力回路27Bの入力結果を読み出し、これと信号入力回路27Aの入力結果との比較照合を行う。この照合結果は故障診断回路26Aに送られ、これに基づき故障診断回路26Aは故障診断を行う。コントローラ1B内の比較照合回路28B及び故障診断回路26Bも同様の動作を行う。この場合は、比較照合回路28A、28Bの照合結果は一致し、従って故障診断回路26A、26Bはいずれも正常である旨の診断を行う。

【0042】ところが、入力ユニット8A内のフォトトランジスタ22Aが導通故障している場合、実際の入力接点信号S1は“0”にも拘わらず信号入力回路27Aは“1”を入力することになる。この場合のフォトトランジスタ22Aの導通故障は危険側故障であるが、図2の構成によればこのような故障に基づく入力結果を排除することができる。

【0043】すなわち、チェック信号発生回路29Aは、チェック信号としての“0”信号及び“1”信号を定期的に交互に出力している。いま、チェック信号発生回路29Aが“0”信号を発光ダイオード24Aに出力している状態であればフォトトランジスタ25Aはオフ

状態であるため、発光ダイオード21Aには電流が流れず、従ってフォトトランジスタ22Aも必ずオフ状態となるはずである。それにもかかわらず、信号入力回路27Aが“1”を入力しているのはフォトトランジスタ22Aに導通故障が生じていることに他ならない。故障診断回路26Aは、このチェック信号発生回路29Aの出力状態と信号入力回路27Aの入力結果とに基づいて入力ユニット8Aが故障であると判断する。

【0044】一方、チェック信号発生回路29Aが“1”信号を出力している状態の場合は、信号入力回路27Aが“1”を入力したとしてもそれだけでは入力ユニット8Aに故障が生じているか否かは分からない。しかし、この場合、比較照合回路28AがB系との間で照合を行っているので、故障診断回路26Aはこの照合結果によって入力ユニット8Aに故障が生じていることを判断することができる。

【0045】また、入力接点信号S1が“0”である状態でフォトトランジスタ22Aにオープン故障が生じる場合がある。この場合は、チェック信号発生回路29Aの出力信号が“0”又は“1”のいずれであっても信号入力回路27Aは“0”を入力し、正常状態における場合と同様の入力結果を示すため、故障診断回路26Aは正常と判断することになる。つまり、コントローラ1Aは正常と判断しているが実際には故障が潜在した状態となっている。しかし、この故障は既述したように安全側故障であり、直ちに検出されなくても重大事故に直結するものではないため許容され得る看過である。

【0046】図3は、入力ユニットの代表的な故障モードを示した図表である。上述した例は、項目1乃至4に該当する。なお、“0”信号及びこれに続く“1”信号を1組の信号と見た場合には、一見すると、項目1及び項目2、あるいは項目3及び項目4を一つの項目として表記することも可能であるように思える。しかし、入力ユニットの正常・故障状態は瞬時に変化する可能性を有することから、フェイルセーフ機能を追求するためには、チェック信号発生回路29Aが“0”信号を出力した時点及び“1”信号を出力した時点の各時点において単独で正常又は故障の判断を行う必要がある。それ故、図3においては、項目1、2、項目3、4、…項目19、20等をそれぞれまとめて表記せず、単独の項目として表記している。

【0047】図4は、図1における出力ユニット9A、9Bの構成と、この出力ユニット9A、9Bとの間で信号の授受を行うマイクロプロセッサ・コントローラ1A、1Bの構成とを示すブロック図である。この図において、出力ユニット9Aは、発光ダイオード31A及びフォトトランジスタ32Aにより形成されるフォトカプラ30A（出力用半導体素子）と、発光ダイオード34A及びフォトトランジスタ35Aにより形成されるフォトカプラ33A（故障検出用半導体素子）と、発光ダイ

(8)

オード37A及びフォトランジスタ38Aにより形成されるフォトカプラ36A(チェック用半導体素子)と、抵抗39Aとを有している。出力ユニット9Bも出力ユニット9Aと同様の構成を有しているが、その他に、ダイオード40及び抵抗41を有している。

【0048】コントローラ1Aは、出力信号駆動回路42Aと、故障検出回路43Aと、チェック信号発生回路44Aと、接点リードバック回路45Aとを有している。そして、コントローラ1Bもコントローラ1Aと同様の構成を有している。また、図1においても示したリレー17及びリレー接点18は、遮断機制御装置などの現場機器内に配設されている。

【0049】24ボルト電源の高圧側端子には直列接続されたヘルシーリレー接点14A、14Bを介してフォトカプラ30Aが接続されており、これに続いてフォトカプラ30B、ダイオード40を介してリレー17の一端側が接続され、リレー17の他端側が24ボルト電源の0ボルト端子に接続されている。したがって、出力ユニット9Aの信号出力経路と、出力ユニット9Bの信号出力経路とは互いに直列接続されている。

【0050】リレー17に対して励磁信号としての“1”信号が出力ユニット9A及び9Bから同時に出力されてリレー17が励磁されている状態では、リレー接点18が閉じ、遮断機が上がった状態となっている。また、リレー17に対して無励磁信号としての“0”信号が出力ユニット9A及び9Bから出力されてリレー17が無励磁の状態になっていれば、リレー接点18が開き、遮断機が下がった状態になっている。したがって、出力ユニットのフェイルセーフ性とは、“0”信号を出力して遮断機を下げていなければならない場合にもかかわらず、誤って“1”信号が出力され遮断機を上げてしまうような故障を確実に防止することである。図4の出力ユニットの構成は、図2の入力ユニットの場合と同様に、“1”信号を危険側信号、“0”信号を安全側信号として扱い、危険側故障に起因する事故を確実に防止するためのものである。

【0051】次に、図4の動作につき説明する。A系及びB系のいずれも正常に機能している場合はヘルシーリレー接点14A、14Bの双方がオンになっている。いま、出力信号駆動回路42A、42Bの一方又は双方から“0”信号が出力されていれば、フォトランジスタ32A、32B及びダイオード40の経路には電流が流れないので、リレー17は無励磁状態であり、したがって遮断機は下がった状態となっている。このとき、リレー接点18はオフとなっており、接点リードバック回路45A、45Bは“1”信号を検出する。一方、出力信号駆動回路42A、42Bの双方から“1”信号が出力されていれば、フォトランジスタ32A、32B及びダイオード40の経路に電流が流れるので、リレー17は励磁状態となり、したがって遮断機は上がった状態と

なる。このとき、リレー接点18はオンとなり、接点リードバック回路45A、45Bは“0”信号を検出する。

【0052】そして、上記のように、フォトランジスタ32A、32B及びダイオード40の経路に電流が流れていない状態では、抵抗39A、発光ダイオード34A側及び抵抗39B、発光ダイオード34B側にそれぞれ微弱電流が流れ、故障検出回路43A、43Bが

“1”信号を入力するようになっている。一方、フォトランジスタ32A、32B及びダイオード40の経路に電流が流れている状態では、抵抗39A、発光ダイオード34A側及び抵抗39B、発光ダイオード34B側に微弱電流は流れず、故障検出回路43A、43Bは“0”信号を入力するようになっている。

【0053】上記の故障検出回路43A、43Bによりフォトランジスタ32A、32Bの故障を検出することができる。すなわち、例えば、フォトランジスタ32Aが導通故障している場合には、出力信号駆動回路42Aから“0”信号が出力されているにもかかわらず、故障検出回路43Aが“0”信号を入力する(正常であれば、回路43Aは“1”信号を入力するはずである)。したがって、フォトランジスタ32Aの導通故障を検出することができる。また、フォトランジスタ32Aがオープン故障している場合には、出力信号駆動回路42Aから“1”信号が出力されているにもかかわらず、故障検出回路43Aが“1”信号を入力する(正常であれば、回路43Aは“0”信号を入力するはずである)。したがって、フォトランジスタ32Aのオープン故障を検出することができる。

【0054】上記のように、フォトカプラ33A及び故障検出回路43Aによりフォトランジスタ32Aの故障を検出できるようになっている。しかし、フォトカプラ33Aのフォトランジスタ35Aが故障した場合、特に、その故障が導通故障である場合はフェイルセーフ性を維持することができなくなる。なぜなら、フォトランジスタ35Aが導通故障している場合は故障検出回路43Aの入力が常時“1”となるため、フォトランジスタ32Aに導通故障が生じ、危険側信号である“1”信号が誤ってリレー17に出力されても、これを検出することができなくなるからである(これに対し、フォトランジスタ35Aのオープン故障の場合は、故障検出回路43Aの入力が常時“0”となり、コントローラ自体がリレー17に危険側信号である“1”信号が出力されていることを認識していることになるので重大事故に直結することはない)。したがって、フェイルセーフ性を確保するためには、フォトランジスタ35Aの導通故障は確実に検出すべき事象である。フォトカプラ36A及びチェック信号発生回路44Aは、この確実に検出すべき事象であるフォトランジスタ35Aの導通故障を検出するために設けられたもの

(9)

であり、チェック信号発生回路44Aは定期的に“0”信号及び“1”信号を交互に出力している。

【0055】すなわち、チェック信号発生回路44Aはチェック信号としての“1”信号及び“0”信号を交互に発光ダイオード37Aに出力し、フォトトランジスタ38Aをオンオフする。これにより、発光ダイオード34Aに流れる電流が強制的にオンオフされる。したがって、故障検出回路43Aが“1”信号を入力した状態でチェック信号発生回路44Aがチェック信号を出力した場合に、このチェック信号に応じて故障検出回路43Aの信号入力状態が変化せず、連続して“1”信号を入力している状態となっているのであれば、それはフォトトランジスタ35Aに導通故障が発生しているからであるということが分かる。

【0056】図5は、出力信号駆動回路42A、接点リードバック回路45A、チェック信号発生回路44A、及び故障検出回路43Aの動作を説明するためのタイムチャートであり、(a)は正常動作の場合、(b)は危険側故障の場合、(c)は安全側故障の場合をそれぞれ示している。なお、「出力されるべき信号」とは、リレー17に対して本来正しく出力されるべき信号の意味である。

【0057】図5(a)に示されるように、正常の場合には、故障検出回路43Aが入力する信号は、チェック信号発生回路44Aが“0”信号を出力している場合には必ず“0”であり、また、チェック信号発生回路44Aが“1”信号を出力している場合には接点リードバック回路45Aが読み取った信号と同じ信号となっている。

【0058】しかし、図5(b)に示されるように、フォトトランジスタ35Aに導通故障が生じた場合は、チェック信号が“0”であるにもかかわらず故障検出回路43Aは“1”信号を入力している。そのため、この時点で直ちにシステムを停止させて危険側故障に起因する重大事故の発生を未然に防止するようにしている。もし、この時点でシステムを停止させずにそのまま運転を継続した場合、フォトトランジスタ32Aに導通故障が生じて、これを検出することができなくなるからである。

【0059】また、図5(c)に示されるように、フォトトランジスタ35Aにオープン故障が生じた場合は、接点リードバック回路45Aが“0”信号を読み取っている期間は、チェック信号の変化によってもこのオープン故障は検出されることがない。しかし、既述した通り、この期間中にフォトトランジスタ35Aのオープン故障が検出できなくとも重大事故に直結することはない。そして、この状態のままフォトトランジスタ32Aにオープン故障が発生すると、チェック信号が“1”であるにもかかわらず故障検出回路43Aが入力する信号が“0”となり、接点リードバック回路45Aの信号と

一致しないために、フォトトランジスタ32Aのオープン故障が検出され、システムが停止されることになる。図6に、上述したような故障を含めた、出力ユニットの代表的な故障モードを示す。

【0060】ところで、図4におけるフォトトランジスタ32A、32Bは特異な状態に陥る可能性を有するものである。特異な状態とは、例えば、出力信号駆動回路42Aが“0”信号を出力している場合に、フォトトランジスタ32Aが不飽和の状態でその漏れ電流を増加させ、リレー17を励磁してしまう虞れのあるレベルの電流を流している状態のことをいう（この状態のことを「半導通状態」と呼ぶ。）。この半導通状態では、リレー17は実際には励磁されておらず、故障検出回路43Aも“1”信号を入力しているので何らの故障も検出されていない。しかし、フォトトランジスタ32Aがこのような半導通状態に陥っている間にフォトトランジスタ32Bに導通故障が生じると、出力信号駆動回路42A、42Bが“0”信号を出力しているにもかかわらずリレー17が励磁されてしまい、出力ユニット9A、9Bのフェイルセーフ性が失われることになる。重大事故の発生を確実に防ぎ安全性を向上させるためには、このような半導通状態が生じていることを確実に検出し、速やかにシステムを停止させてフェイルセーフ性を維持することが求められる。図4の構成によれば、このような半導通状態を確実に検出することが可能である。

【0061】すなわち、正常の状態において出力信号駆動回路42Aが“0”信号を出力している場合には、微弱電流が抵抗39A、発光ダイオード34A、フォトトランジスタ38Aを通して出力ユニット9B側に出力されるが、この出力される微弱電流はチェック信号発生回路44Aの働きによって“0”と“1”とが交互に繰り返される信号となっている。したがって、チェック信号発生回路44Bの出力によりフォトトランジスタ38Bがオンになっている状態において、故障検出回路43Bは、出力ユニット9A側からの信号が“1”の場合には“1”信号を入力し、出力ユニット9A側からの信号が“0”の場合には“0”信号を入力するはずである。ところが、フォトトランジスタ32Aが上記の半導通状態に陥っている場合には、その漏れ電流によって出力ユニット9Aからの電流レベルが上昇し、故障検出回路43Bは、フォトトランジスタ38Bがオンになっている状態においては常時“1”信号を入力することになる。この現象により、フォトトランジスタ32Aが半導通状態にあることを検出することができる。上記の例は、A系側のフォトトランジスタ32Aが半導通状態にあることをB系側の故障検出回路43Bの入力状態に基づいて判別していたが、B系側のフォトトランジスタ32Bに半導通状態が生じている場合もA系側の故障検出回路43Aの入力状態に基づいて判別することができる。

【0062】次に、図1において示したヘルシー回路1

0A, 10Bにつき説明する。図7は、このヘルシー回路10A, 10Bの構成図である。図7においてA系を例に取り説明すると、コントローラ1Aのマイクロプロセッサ・ユニット2Aは交番信号を生成するが、この交番信号は入出力インタフェイス5A及びI/Oバス7Aを介してヘルシー回路10Aに送出される。そして、ヘルシー回路10Aでは、出力回路11Aがこの交番信号をトランス12Aの1次側に出力し、その2次側からは直流分がカットされて交番信号の交流分のみが出力される。トランス12Aの2次側から出力される交番信号はダイオード46Aにより整流され、この整流された電流によってリレー13Aが励磁され、ヘルシーリレー接点14Aがオンとなる。

【0063】上記したように、リレー13Aは間接的にはマイクロプロセッサ・ユニット2Aによって生成される交番信号に基づき励磁されるので、マイクロプロセッサ・ユニット2Aが故障を検知した場合には必ず無励磁となってヘルシーリレー接点14Aがオフとなる。つまり、マイクロプロセッサ・ユニット2Aが故障を検知した場合、通常、マイクロプロセッサ・ユニット2Aは全ての出力をクリアして“0”とするが、故障の種類によっては出力をクリアできなくなることがある。そして、マイクロプロセッサ・ユニット2Aから出力回路11Aに対して“1”信号が出力され続けることになるが、この場合には出力回路11Aがトランス12Aの1次側に供給する信号が交番信号ではなくなり、トランス12Aの2次側出力はゼロとなるためリレー13Aが励磁されることはない。したがって、マイクロプロセッサ・ユニット2Aが故障を検知した場合にはリレー13Aは必ず無励磁となってヘルシーリレー接点14Aをオフの状態にすることができる。そして、図4において図示したように、ヘルシーリレー接点14A, 14Bは直列接続された状態で電源回路に接続されているので、いずれか一方がオフになった場合には決して現場機器内のリレー17が励磁されることがない。

【0064】図8は、出力回路11A, 11Bの信号出力状態とリレー13A, 13Bの励磁状態を示すタイムチャートである。この図において、当初A系及びB系共に正常に機能していたが、ある時点でA系のマイクロプロセッサ・ユニット2Aが故障を検知したとする。すると、マイクロプロセッサ・ユニット2Aは直ちに全ての出力をクリアするため出力回路11Aからの交番信号の出力は停止され、それまで励磁状態となっていたリレー13Aは無励磁状態となる。そして、B系のマイクロプロセッサ・ユニット2Bは、A系のマイクロプロセッサ・ユニット2Aが交番信号の生成を停止したことを照合機能によって検知できるようになっている。したがって、マイクロプロセッサ・ユニット2Bも、この後すぐに交番信号の生成を停止する。これにより、出力回路11Bからの交番信号の出力も停止されリレー13Bも無

励磁状態となる。

【0065】ここで、上記の交番信号において“1”となっている時間及び“0”となっている時間を一定に保つための技術につき説明する。交番信号を出力する場合、通常は、マイクロプロセッサ・ユニット2Aがメインプログラムで出力することが考えられる。しかし、マイクロプロセッサ・ユニット2Aの処理が正常に行われている間はメインプログラムの制御処理時間が一定であるため特に問題は生じないが、外部からの入力信号の入力状況如何によってはこの制御処理時間が一定でなくなり、“1”である時間及び“0”である時間を一定に保つことが困難になる。

【0066】そこで、本実施形態では、図9に示すように、マイクロプロセッサ・ユニット2A内にメインプログラムを実行する制御処理手段47の他に、割り込みプログラムを実行する交番信号発生手段48を設け、これにより交番信号を発生させるようにしている。制御処理手段47はカウンタ49及び走行フラグ50を有しており、交番信号発生手段48はカウンタ51を有している。

【0067】このような構成によりフェイルセーフな交番信号を発生させるためには、メインプログラムに異常が生じた場合は、割込プログラムによって確実にその走行を停止させて交番信号の発生を停止させる必要がある。一方、割込プログラムに異常が生じた場合も、メインプログラムによって確実にその走行を停止させて交番信号の発生を停止させる必要がある。そして、交番信号の周期はできるだけ短い方が望ましいが、割込プログラムが余りに頻繁に走行するとメインプログラムでの処理時間がなくなってしまうので、その周期は適切に選ぶ必要がある。図9の例では、制御処理手段47が実行するメインプログラムの1回の処理時間を100～200msとし、交番信号発生手段48が実行する割込プログラムの割込周期を5msとする。したがって、正常状態であれば、メインプログラムの1回の処理時間の間に割込プログラムが20～40回走行することになる。この関係を利用してヘルシー回路の交番信号を発生させることができる。

【0068】次に、図9の動作につき説明する。なお、この例では、メインプログラムの1回の処理時間を100msとし、正常な割込回数を20±1回とする。制御処理手段47は、1回の走行開始時に走行フラグ50をセットすると共にカウンタ49に走行回数についてのカウント値を加算し、更に1回の走行終了時に走行フラグ50をリセットする。一方、交番信号発生手段48は、走行フラグ50がセットされると5ms毎の割込を走行フラグ50がリセットされるまで行い、“1”又は“0”の交番信号を発生させる。そして、交番信号発生手段48は、このときの割込回数についてのカウント値をカウンタ51に加算する。

【0069】制御処理手段47が1回の走行を終了して走行フラグ50をリセットし、次の走行を行うべく再度走行フラグ50のセットを行うと、この時点で交番信号発生手段48は、カウンタ51のカウンタ値をチェックする。いま、カウンタ51のカウンタ値が22回であったとすると、制御処理手段47は、メインプログラムに異常が発生していると判別し、全プログラムの走行を停止させる。

【0070】一方、制御処理手段47の側でもこの時点でカウンタ51のカウンタ値をチェックしている。したがって、交番信号発生手段48側に何らかの異常が発生し、その結果カウンタ51のカウンタ値が22回になった場合であっても、制御処理手段47は、割込異常として全プログラムの走行を停止させることができる。

【0071】なお、制御処理手段47は、上記の割込異常以外の異常（例えば、B系側の入力データとの照合結果が一致しない等の異常）が生じた場合は、図示を省略してあるエラーフラグをセットして全プログラムを停止させる。このエラーフラグについては、交番信号発生手段48もチェックしており、エラーフラグがセットされると直ちに割込プログラムの走行を停止し、交番信号の発生を停止するようになっている。

【0072】上記した図9の構成によれば、メインプログラム側が何らかの原因で処理時間がかかる故障を起こした場合、あるいは処理時間が余りに短いような故障を起こした場合に、メインプログラム自身がこれらの故障を検出できないときでも、割込プログラムにより故障を検出してヘルシーリレーを無励磁にすることができる。また、割込プログラム側が割込頻度が異常に高い故障又は異常に低い故障を起こした場合は、これをメインプログラムで検出してヘルシーリレーを無励磁にすることができる。すなわち、高速で且つ高精度の周期を有する交番信号を出力することができ、フェイルセーフを実現することができる。さらに、交番信号を高速化することができるため、ヘルシー回路10A、10B内のトランス12A、12Bを小型化することができ、速い応答性を得ることができるようになる。

【0073】次に、図1に示した共有メモリ16A、16Bの利用により、プログラムの内容の一部を効率的に書き換える技術につき説明する。一般に、電子踏切制御装置のプログラムには標準的なものが用意されているが、タイマ等の定数については現場の踏切の実際の状況に合わせる必要があるため、予めインストールされているプログラムの内容の一部を変更して使用する場合が通常である。このようなプログラム内容の変更は、電子踏切制御装置を実際に設置する際や、設置後の運用結果に基づいて行われることが多いが、いずれにしても現場において行わなければならないので、この変更処理は容易且つ確実に実行できるようにしておくことが望ましい。本実施形態の構成によれば、共有メモリの働きにより、

A系又はB系のいずれか一方の系のみに対してプログラム内容の一部を変更すれば、他方の系のプログラム内容も自動的に変更されるようにすることができる。

【0074】すなわち、現場にいるオペレータは、図1においては図示を省略してあるPC（パーソナル・コンピュータ）モニタを操作して、変更すべきタイマ等の定数をマイクロプロセッサ・ユニット2Aを介して記憶部3Aに書き込む。この記憶部3Aは、既述したように、EEPROMにより形成されているので、電氣的な書込が可能であり、また、電源が停電した場合でもデータ保持が可能なものである。

【0075】記憶部3Aに書き込まれたデータは共有メモリ16Aにも書き込まれるが、B系マイクロプロセッサ・コントローラ1Bはこの共有メモリ16Aの内容を読み出し、これを自系の記憶部3B及び共有メモリ16Bに書き込む。そして、A系マイクロプロセッサ・コントローラ1Aは、共有メモリ16Aのデータと共有メモリ16Bとを照合し、その照合結果をPCモニタに出力する。PCモニタは、A系に書き込まれたデータと、A系への書込に伴ってB系に書き込まれたデータとを比較し、両者が一致していれば正常である旨を表示し、また、不一致であればA系の動作を停止するようにA系マイクロプロセッサ・コントローラ1Aに指示する。なお、変更データの信頼性を高めるために、定数データにはデータの誤りを検出できるチェックコードと一緒に送信することも可能である。

【0076】このように、図1の構成によれば、タイマ等の定数などを変更する場合、2台のマイクロプロセッサ・コントローラのうち1台のみに対して変更処理を行えば、他方の系の定数も自動的に変更される。そして、自系と他系の変更内容が同一になっているか否かについてのチェックも同時に実行することができるので、人間の操作ミスによる誤った定数の設定を防止することができる。

【0077】次に、本発明の第2の実施形態につき説明する。図10はこの第2の実施形態の構成を示すブロック図である。図1に示した第1の実施形態は、A系（第1の制御系）及びB系（第2の制御系）の2つの制御系を有するものであったが、この第2の実施形態は3つの制御系を有するものであり、A系及びB系の2つの制御系の他にさらにC系（第3の制御系）を有するものである。そして、図11は、この図10に示した電子踏切制御装置を用いて構成した電子踏切制御システムの構成図である。

【0078】まず、図11の電子踏切制御システムについて先に説明する。この図において、第1の制御処理端末装置61、第2の制御処理端末装置62、及び4台の入出力処理端末装置63～66の各制御系は、A～C系のLANによって互いに接続されている。そして、入出力処理端末装置63～66は、それぞれ現場機器67～

70との間で信号の授受を行うようになっている。

【0079】第1の制御処理端末装置61及び第2の制御処理端末装置62は入出力処理端末装置63～66の上位機器であり、現場機器67～70は実質的にはこれら第1の制御処理端末装置61又は第2の制御処理端末装置62により、入出力処理端末装置63～66を介して制御されることになる。

【0080】第1の制御処理端末装置61には現在の列車運行に用いられるプログラムが実装されており、第2の制御処理端末装置62には新しく開発された応用プログラムが実装されている。そして、列車運行数が多い時間帯（昼間）には全ての現場機器67～70が稼働するが、列車運行数が少ない時間帯（夜間）には現場機器67のみが稼働し、現場機器68～70に対しては改修工事あるいは試験等が行われるものとする。

【0081】入出力処理端末装置63～66のそれぞれは、第1の制御処理端末装置61又は第2の制御処理端末装置62のうちのいずれと信号の授受を行うかを定める切換スイッチを有しており、この切換スイッチの制御は第2の制御処理端末装置62により行われるようになっている。昼間は、全ての入出力処理端末装置63～66は現場機器67～70からの入力信号を第1の制御処理端末装置61のみに対して出力し、一方、第1の制御処理端末装置61のみが入出力処理端末装置63～66に対して信号を出力する。しかし、夜間になって第2の制御処理端末装置62が上記の切換スイッチを所定の位置に切り換えると、入出力処理端末装置63のみが現場機器67からの入力信号を第1の制御処理端末装置61に対して出力し、一方、第1の制御処理端末装置61は入出力処理端末装置63のみに対して信号を出力する。そして、入出力処理端末装置64～66は、現場機器68～70からの入力信号を第2の制御処理端末装置62に対して出力し、一方、第2の制御処理端末装置62は入出力処理端末装置64～66に対して信号を出力する。

【0082】このような鉄道用保安制御システムによれば、特定の線路を使用する列車の運行は継続したまま、他の線路に設けられた踏切の改修工事あるいは試験等を行うことが可能になるので、改修工事の効率を大きく向上させることができ、工期の短縮を図ることができる。

【0083】次に、図10の構成につき説明する。この図において、A系のマイクロプロセッサ・コントローラ71Aは、マイクロプロセッサ・ユニット72A、メモリ部73A、LAN制御部74A、及びI/Oバス・インタフェース75Aを有している。マイクロプロセッサ・コントローラ71AはI/Oバス・インタフェース76Aを介して入力ユニット77A、出力ユニット78A、及びヘルシー回路79Aと接続されている（入力ユニット77A及び出力ユニット78A構成は、それぞれ

図2及び図4に示したものと略同様の構成のものである。）。B系及びC系もA系と同様の構成を有している。そして、A系とB系との間には共有メモリ80、B系とC系との間には共有メモリ81、C系とA系との間には共有メモリ82が、それぞれ設けられている。

【0084】各系の入力ユニット77A、77B、77Cには、現場機器入力信号モジュール83を介して現場機器67（又は現場機器68～70）からの信号が入力されるようになっており、また、各系の出力ユニット78A、78B、78Cからの信号が現場機器出力信号モジュール84を介して現場機器67に出力されるようになっている。そして、各系のヘルシー回路79A、79B、79Cからのヘルシーリレー接点信号の状態が、現場機器出力信号モジュール84、さらに現場機器入力信号モジュール83に対して送出されるようになっており、3系のうち少なくとも2系が正常でなければ現場機器出力信号モジュール84及び現場機器入力信号モジュール83が動作しないようになっている。なお、現場機器入力信号モジュール83及び現場機器出力信号モジュール84は、図10の構成についての理解を容易にするために概念的な要素として図示したものであり、実際には各コントローラ内のマイクロプロセッサ・ユニット72A、72B、72Cの機能として考えられるものである。

【0085】図12は、図10におけるヘルシー回路79A、79B、79Cの構成図である（ヘルシー回路79B、79Cの構成はヘルシー回路79Aと同様であるため省略する。）。この図において、A系マイクロプロセッサ・コントローラ71Aのマイクロプロセッサ・ユニット72Aは交番信号を生成するが、この交番信号はI/Oバス・インタフェース75A、76Aを介してヘルシー回路79Aに送出される。ヘルシー回路79Aでは、2つの出力回路85A1、85A2がこの交番信号をそれぞれトランス86A1、86A2の1次側に出力し、その2次側からは直流分がカットされて交番信号の交流分のみが出力される。トランス86A1、86A2の各2次側から出力される交番信号はそれぞれダイオード87A1、87A2により整流され、この整流された電流によってリレー88A1、88A2が励磁され、ヘルシーリレー接点89A1、89A2がオンとなる。

【0086】図12のヘルシー回路79Aの動作は、図7の場合と略同様であるため、その重複した説明は省略し、各系間のヘルシーリレー接点のオンオフの組合せのみについて説明する。図12における「ヘルシーA=B、ヘルシーA=C、…ヘルシーC=B」は、他系と関連するヘルシーリレー接点を示している。つまり、イコール記号の左側のアルファベット記号は自系側を示し、イコール記号の右側のアルファベット記号は他系側を示している。

【0087】そして、例えば、A系コントローラが自己

(13)

診断によって自系の故障を検出した場合は、 $A=B$ 及び $A=C$ の接点をオフにして自系の走行を停止する。このとき、B系側では $B=C$ の接点はオンのままにしておくが、A系と関連する接点である $B=A$ の接点をオフにする。同様に、C系側でも $C=B$ の接点はオンのままにしておくが、A系と関連する接点である $C=A$ の接点をオフにする。

【0088】一方、A系コントローラがその照合機能によって他系の故障を検出した場合は、その他系と関連する接点のみをオフにする。例えば、A系コントローラがB系の故障を検出した場合は、 $A=B$ の接点のみをオフにして $A=C$ の接点はオンにしておく。このとき、C系側でもC系コントローラがB系の故障を検出し、 $C=B$ の接点のみをオフにして $C=A$ の接点はオンにしてあるはずである。そして、A系側及びC系側の各接点 $A=B$ 及び $C=B$ がオフになったことにより、B系側の接点 $B=C$ 及び $B=A$ もオフとなり、B系の走行が停止される。

【0089】図10に示した第2の実施形態は、既述したように、A系、B系、C系の3重系構成を有するものであり、そのうち2系の入力データ又は出力データが一致した場合に、その入力データ又は出力データを正常データとして取り扱うとする、所謂「2 out of 3」方式を採用している。3系のうち2系の入出力データが一致する場合の態様としては、次の3つの態様がある。

【0090】(1) A系及びB系のヘルシーリレー接点が共にオン（ヘルシーリレーが励磁状態）であり、且つA系及びB系の出力データ（又は入力データ）が共に“1”である。

(2) B系及びC系のヘルシーリレー接点が共にオン（ヘルシーリレーが励磁状態）であり、且つB系及びC系の出力データ（又は入力データ）が共に“1”である。

(3) C系及びA系のヘルシーリレー接点が共にオン（ヘルシーリレーが励磁状態）であり、且つC系及びA系の出力データ（又は入力データ）が共に“1”である。

【0091】例えば、B系において故障が発生した場合、ヘルシー回路79Bの接点 $B=C$ 及び $B=A$ がオフになると共に、ヘルシー回路79A、79Cの接点 $A=B$ 及び $C=B$ がオフになる。しかし、ヘルシー回路79A、79Cの接点 $A=C$ 及び $C=A$ はオン状態を維持しているので、正常なA系及びC系によってシステムの制御を継続することができる（上記の(3)の態様）。

【0092】次に、図10の動作を、図13のフローチャートに基づき説明する。但し、図13においてはA系及びB系相互間のみの動作を説明し、B系及びC系相互間並びにC系及びA系相互間についての重複した説明を省略する。

【0093】コントローラ71A、71Bは、まず、プログラムで制御を開始するための同期処理を行う。すな

わち、コントローラ71A、71Bは、「同期通番」と呼ばれる処理回数を示す番号を共有メモリ80の自系領域80A、80Bに書き込み、自系の同期通番と他系の同期通番とが一致するか否かを確認することにより同期が取れたか否かを判別する（ステップ101A、101B）。同期が取れない場合は一定時間だけ待ち、それでも同期が取れない場合は互いに他系を故障と判断し、それぞれヘルシーリレー接点をオフにしてヘルシーリレーを無励磁とする。そして、同期が取れた場合は、そのタイミングで制御処理を開始する。

【0094】同期が取れた後、各コントローラは、入力モジュール83を通して入力した現場機器67からの入力信号を読み込み、これを自系の記憶領域80A、80Bに書き込む。そして、自系に書き込んだ入力信号と他系に書き込まれた入力信号とが一致するか否かを判別する（ステップ102A、102B）。一致しない場合は、それぞれ他系を故障と判別し、一方、一致する場合は制御のための演算処理を行う（ステップ103A、103B）。

【0095】各コントローラは、演算処理結果を出力信号として自系の記憶領域80A、80Bに書き込み、さらに自系に書き込んだ出力信号と他系に書き込まれた出力信号とが一致するか否かを判別する（ステップ104A、104B）。一致しない場合は、それぞれ他系を故障と判別し、一方、一致する場合は、これを出力モジュール84を介して現場機器67に出力する。

【0096】このように、A系側コントローラは自系の制御処理を行うと共に、B系側コントローラに対する故障検出器としても機能しており、また、B系側コントローラも自系の制御処理を行うと共に、A系側コントローラに対する故障検出器としても機能している。したがって、現場機器との間で確実な入出力制御を行うことができる。

【0097】図14は、図13において説明した他系との同期チェック処理、入力処理、及び出力処理を含め、エラー処理が行われる主な場合をA系側を例に取って示したフローチャートである。A系コントローラ71Aは、まず、自系のI/Oバス等について異常がないか否かにつき自己診断を行い（ステップ1）、異常があった場合、すでに励振出力されていればエラー処理として励振処理の出力を停止し（ステップ19）、制御動作を停止する（ステップ20）。励振出力とは、図12においてマイクロプロセッサ・ユニット72Aが交番信号の発生し、出力回路85A1、85A2に交番信号を出力させることである。

【0098】コントローラの自己診断の結果、異常がなければ上記の励振出力を行う（ステップ2）。そして、コントローラ71Aは、共有メモリ80、82に対する書き込みテスト及び読み出しテストを行い（ステップ3）、異常があればステップ19の処理を行う。次い

で、入力ユニット77A及び出力ユニット78Aのオフチェックを行って導通故障が生じていないかどうかをチェックし（ステップ4、5）、異常があればステップ19の処理を行う。そして、前回の制御出力のリードバックを行い、異常がないか否かを確認する（ステップ6）。

【0099】ステップ4～6のチェックの結果、異常がなければ、図13において既述したように、他系すなわちB系及びC系との同期を取るようにし（ステップ7）、同期が取れなければステップ19の処理を行う。同期が取れたならば、入力モジュール83からデータを入力し入力処理を開始する（ステップ8）。そして、8ビットの反転データを作成して、これを共有メモリ80、82に書き込むと共に（ステップ9）、B系及びC系の反転データと照合することにより、これら他系と共有しているメモリデータのチェックを行い（ステップ10）、異常があればステップ19の処理を行う。次いで、入力モジュール83から入力した入力信号について他系と一致するか否かを共有メモリ80、82を用いて照合し（ステップ11）、異常があればステップ19の処理を行う。

【0100】上記の照合の後、2つの同一内容のプログラムである制御処理1、2をメモリエリアと時間を変えて実行する（ステップ12、13）。そして、制御処理1、2による演算結果を照合した結果（ステップ14）、一致しなければ異常であるとしてステップ19の処理を行う。

【0101】この後、この演算結果を出力しようとする前に、ステップ9、10と同様に、反転データの作成及び書き込み並びに他系の反転データとの照合を行い（ステップ15、16）、異常があればステップ19の処理を行う。次いで、出力モジュール84から出力すべき出力信号について他系と一致するか否かを共有メモリ80、82を用いて照合し（ステップ17）、異常があればステップ19の処理を行う。そして、異常がなければ、出力処理を行い（ステップ18）、ステップ1以下の動作を繰り返す。

【0102】A系コントローラはステップ19で励振出力を停止する場合において、自系の異常を検出したときは、 $A=B$ 及び $A=C$ の双方のヘルシーリレー接点をオフにし、B系（又はC系）の異常を検出したときは、 $A=B$ のみ（又は $A=C$ のみ）のヘルシーリレー接点をオフにする。そして、 $A=B$ 及び $A=C$ の双方のヘルシーリレー接点がオフになった場合、A系コントローラは走行を停止するが（ステップ19）、 $A=B$ のみ（又は $A=C$ のみ）のヘルシーリレー接点がオフになった場合は、C系（又はB系）との間で制御処理を続行する。

【0103】上述したように、3系のうちの1つの系に故障が発生した場合、その系のコントローラは自系のヘルシーリレーを無励磁にして自系の走行を停止させるよ

うになっているが、もし、自系のヘルシーリレーを無励磁にできなかったとしても、他の2系が故障系のヘルシーリレーを無励磁にし、故障系を制御処理に参加させないようにしてシステムの安全性を確保している。しかし、故障系を除いた他の2系で制御処理を続行している間に、何らかの原因で故障系が再び制御処理に参加するような事態が生じるとシステムの安全性が阻害されることになる。そこで、本実施形態では、このような事態が生じることのないように、故障系の電源回路をオフにし、故障系を他の2つの健全な系から強制的に切断するようにしている。

【0104】図15は、電源回路をオフにする系を各態様毎に示した図表である。なお、この電源回路は、図10においては図示を省略してあるが、各系のコントローラ71A、71B、71C内に設けられているものである。図15において、「0」は故障と判断された系又はその関連する系のヘルシーリレー接点（オフにされるべき接点）であり、「1」は正常な系のヘルシーリレー接点であることを示している。また、X1は故障のために既に電源回路がオフされている系のヘルシーリレー接点（当然、オフになっている）を示し、X2はX1に係るヘルシーリレー接点に追従してオフになっているヘルシーリレー接点を示している。

【0105】したがって、項目1は、3系で制御中にA系が故障したため、まずA系の接点 $A=B$ 及び $A=C$ をオフにすると共に、B系及びC系の接点 $B=A$ 及び $C=A$ をオフにし、A系の電源回路をオフにしてB系及びC系で制御処理を続行する場合を示している。項目2は、C系が故障のため既に電源回路がオフされており、A系及びB系の2系で制御処理を行っている間に、今度はA系が故障したため、A系の電源回路をオフにし、結局B系の電源回路もオフにすべき場合を示している。項目3は、B系が故障のため既に電源回路をオフされており、A系及びC系の2系で制御処理を行っている間に、今度はA系が故障したため、A系の電源回路をオフにし、結局C系の電源回路もオフにすべき場合を示している。

【0106】図16は、故障した系の電源回路を強制的にオフする構成をA系を例に取って示した説明図である。この図において、24ボルトの電源回路の0V端子と24V端子との間にオンタイマリレー90が接続されており、また、複数の接点により形成される接点群とA系電源リレー91との直列接続体も両端子間に接続されている。

【0107】上記の複数の接点とは、オンタイマリレー90のリレー接点92、A系電源リレー91のリレー接点93、 $B=A$ のヘルシーリレー接点94、 $A=B$ のヘルシーリレー接点95、 $C=A$ のヘルシーリレー接点96、 $A=C$ のヘルシーリレー接点97である。また、A系電源リレー91は交流100ボルト電源の主接点98を有している。

【0108】次に、図16の動作を説明する。電源回路の投入時にはオンタイマリレー90が数秒間励磁され接点92をオンにするため、A系電源リレー91が強制的に励磁される。これにより接点93がオンになり、また主接点98がオンとなって、交流100ボルトがコントローラに供給される。そして、A系コントローラは接点95、97をオンにするが、これと同時にB系及びC系のコントローラも動作を開始して接点94、96をオンにする。したがって、A系電源リレー91の自己保持回路が形成され、オンタイマリレー90が無励磁となった後もA系電源リレー91の励磁状態が保持される。

【0109】この状態でB系及びC系がA系の故障を検出すると、接点94、96がオフとなるため、A系電源リレー91は無励磁となり主接点98がオフとなって、故障系であるA系は健全系であるB系及びC系から完全に切断される。また、A系及びB系の2系で制御処理中（C系が故障であるため、接点96、97は既にオフとなっている。）にB系がA系の故障を検出すると、接点94がオフとなるため、A系電源リレー91は無励磁となり主接点98がオフとなって、故障系であるA系の制御は停止される（これに伴って、健全系であるB系の制御も結局は停止される。）。同様に、A系及びC系の2系で制御処理中（B系が故障であるため、接点94、95は既にオフとなっている。）にC系がA系の故障を検出すると、接点96がオフとなるため、A系電源リレー91は無励磁となり主接点98がオフとなって、故障系であるA系の制御は停止される（これに伴って、健全系であるC系の制御も結局は停止される。）。さらに、3系で制御処理中にA系が自己診断により自系の故障を検出した場合は、接点95、97がオフとなるため、この場合もA系電源リレー91が無励磁となってA系の制御が停止される。

【0110】図17は、各リレーの励磁状態及び各ヘルシーリレー接点のオンオフ状態の変化を示すタイムチャートであり、(a)は3系で正常動作中にA系が異常となった場合、(b)はA系及びB系の2系で動作中にA系が異常となった場合を示している。

【0111】図17(a)において、電源投入後に直ちにオンタイマリレー90がオンになると共にA系電源リレー91及びC系電源リレーがオンとなっている。そして、オンタイマリレー90がオフとなった後、B系及びC系がA系の異常を検出したため接点94、接点96がオフとなってA系電源リレー91をオフにする。さらに、この後A系の接点95、97もオフとなる。

【0112】図17(b)において、先にC系の異常が検出され、C系電源リレーがオフとなった後（接点96、97も既にオフとなっている。）、B系がA系の異常を検出し、接点94をオフにしてA系電源リレー91をオフにしている。そして、この後A系の接点95もオフとなる。

【0113】次に、各系のコントローラが他系との間で照合動作を行う場合に、各系のタイマ同士の間におけるカウントタイミングのずれに起因する照合エラーを排除するための技術について説明する。

【0114】各系の基本クロック信号は互いに独立に生成されているので、各系のコントローラのタイマ同士の間では、1カウント分の時間差が発生し、タイマ処理状態が一致しない期間が存在する。例えば、メインプログラムにおいて、所定の基準時点から3秒経過後に或る動作を実行するように設定されている場合を考えてみる。この場合、A系及びB系はそれぞれのタイマが「3」を表示した時点で、既述した入力又は出力の照合を行い、照合結果が一致した場合に上記の動作を実行することになる。

【0115】ところが、A系及びB系の各タイマはそれぞれ独立して時間をカウントしているため、A系タイマが「3」秒を表示した時点では、B系タイマはまだ「2」秒を表示しているという場合があり得る。両タイマはそのカウント値が3.0～3.9秒の期間に「3」秒を表示するようになっているが、例えば、A系タイマが3.7秒をカウントした時点でようやくB系タイマが3.0秒をカウントした状態であったとすると、A系タイマが3.0～3.6秒をカウントしている期間中は、A系タイマは「3」秒を表示し、一方、B系タイマは「2」秒を表示していることになる。したがって、A系タイマが「3」秒を表示した時点で上記の動作を実行すべく両系の照合を行うと、その照合結果は不一致となるため故障と判別されてしまうことになる。

【0116】図18は、このような両系のタイマのずれに起因する誤検知を防止する技術についての説明するためのタイムチャートである。この図において、(a)、(b)はそれぞれA系タイマ及びB系タイマの処理状態を示す信号であり、CA1、CA2…、CB1、CB2…は1回目、2回目、…のカウントを示している。(c)、(e)はスキャン番号が付されたスキャン信号S1～S9を示している。(d)、(f)はA系タイマ及びB系タイマの実際の照合時における処理状態を示す信号TA1、TB1である。(g)は上記の(d)、(f)の信号の一致状態及び不一致状態を示す信号である。また、t1はタイマの1カウントの間隔を示す時間であり、t2はA系タイマとB系タイマの動作開始時点の差を示す時間であり、t3は制御処理周期（スキャン周期）すなわちメインプログラムの走行周期を示している。

【0117】図18(a)、(c)から明らかなように、A系タイマの信号CA2が「1」になっている状態が検出されるのはスキャン信号S3の立ち上がり時点からであり、それ故、実際の照合時におけるA系タイマの処理状態は図18(d)の信号TA1によって示される。同様に、図18(b)、(e)から明らかなように、B系タイマの信号CB3が「1」になっている状態

(16)

が検出されるのはスキャン信号S5の立ち上がり時点からであり、それ故、実際の照合時におけるB系タイマの処理状態は図18(f)の信号TB1によって示される。そして、図18(g)に示されるように、信号TA1, TA2はスキャン信号S3, S4の期間においては互いに不一致の状態となっている。

【0118】したがって、もし上記のスキャン信号S3, S4の期間においてA系とB系との照合を行った場合には、両系のタイマ処理状態が一致しないために照合エラーとなって、故障を検知したと判断されてしまうことになる。しかし、この場合は実際にA系又はB系に故障が発生したわけではなく、上記の故障検知は誤検知である。

【0119】そこで、本実施形態ではこのような誤検知を防止するために、両系のタイマの処理状態の不一致を検出したとしても、所定時間の間はこの不一致を無効とする制御処理を行うようにしている。図18の例では、タイマの1カウントの時間 t_1 がスキャン周期 t_3 よりも大きいので、少なくとも1カウント時間だけ待たないと、両系のタイマの処理状態は確実に一致状態とならない。例えば、 t_1 を100ms、 t_3 を40msとした場合に、3スキャンの間(S3, S4, S5)は不一致を検出したとしてもこの不一致を無効とする処理を行い、4スキャン連続で(S3~S6)不一致を検出した場合にはじめてこの不一致を有効とする処理を行うようにしている。図18の例では、タイマの1カウントの時間 t_1 がスキャン周期 t_3 よりも大きい場合につき説明したが、 t_1 が t_3 よりも十分に小さい場合は、1スキャン時間だけ待てば両系のタイマの処理状態は一致した状態となる。

【0120】

【発明の効果】以上のように、本発明によれば、各制御系が、現場機器との間の信号の入出力結果について、自系統側と1つの他系統側との間で一致するか否かについて共有メモリを用いて照合する機能を有し、全ての制御系の照合結果の組合せが所定の場合にのみ前記現場機器に対する制御を実行するようにしており、また、自系統側又は照合相手の他系統側が正常状態又は故障状態のいずれにあるかをヘルシー回路を用いて検知する機能を有し、いずれかの系統のヘルシー回路から故障信号を入力した場合は制御動作を停止するようにしているので、簡単な構成によって、フェイルセーフ性を向上させることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態の構成を示すブロック図。

【図2】図1における入力ユニット8A, 8B、及びこの入力ユニットと信号の授受を行うA系コントローラ1A, B系コントローラ1Bの構成を示すブロック図。

【図3】図2の入力ユニットの代表的な故障モードを示

した図表。

【図4】図1における出力ユニット9A, 9B、及びこの出力ユニットと信号の授受を行うA系コントローラ1A, B系コントローラ1Bの構成を示すブロック図。

【図5】図4の動作を説明するためのタイムチャート。

【図6】図4の出力ユニットの代表的な故障モードを示す図表。

【図7】図1におけるヘルシー回路10A, 10Bの構成図。

【図8】図8の動作を説明するためのタイムチャート。

【図9】図7におけるマイクロプロセッサ・ユニット2Aの構成を示すブロック図。

【図10】本発明の第2の実施形態の構成を示すブロック図。

【図11】図11の実施形態に係る電子踏切制御装置（鉄道用保安制御装置）を用いて構成した電子踏切制御システム（鉄道用保安制御システム）の構成図。

【図12】図10におけるヘルシー回路79A, 79B, 79Cの構成図。

【図13】図10の動作を説明するためのフローチャート。

【図14】図10のエラー処理が行われる主な場合を説明するためのフローチャート。

【図15】図10における各系のコントローラ内の電源回路をオフにする場合の態様を示す図表。

【図16】図10における各系のコントローラ内の電源回路をオフにするための構成図。

【図17】図16の動作を説明するためのタイムチャート。

【図18】図10における各系のコントローラが他系との間で照合動作を行う場合に、各系のタイマ同士の間におけるカウントタイミングのずれに起因する照合エラーを排除するための技術を説明するためのフローチャート。

【図19】従来の鉄道用保安制御装置の要部の構成を示すブロック図。

【符号の説明】

1A, 1B A系及びB系マイクロプロセッサ・コントローラ

2A, 2B マイクロプロセッサ・ユニット

3A, 3B 記憶部

4A, 4B 記憶部

5A, 5B 入出力インタフェース

6A, 6B MPUバス

7A, 7B I/Oバス

8A, 8B 入力ユニット

9A, 9B 出力ユニット

10A, 10B ヘルシー回路

11A, 11B 出力回路

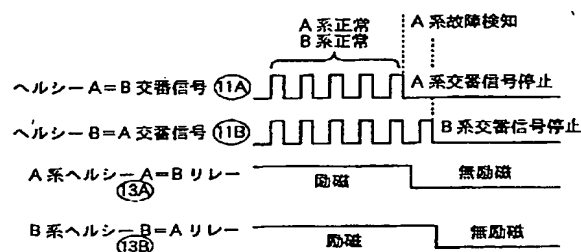
12A, 12B トランス

(17)

13 A, 13 B リレー
 14 A, 14 B ヘルシーリレー接点
 15 A, 15 B I/Oバスコントローラ
 16 A, 16 B 共有メモリ
 17 リレー
 18 リレー接点
 19 A, 19 B 抵抗
 20 A, 20 B フォトカプラ
 21 A, 21 B 発光ダイオード
 22 A, 22 B フォトトランジスタ
 23 A, 23 B フォトカプラ
 24 A, 24 B 発光ダイオード
 25 A, 25 B フォトトランジスタ
 26 A, 26 B 故障診断回路
 27 A, 27 B 信号入力回路
 28 A, 28 B 比較照合回路
 29 A, 29 B チェック信号発生回路
 30 A, 30 B フォトカプラ
 31 A, 31 B 発光ダイオード
 32 A, 32 B フォトトランジスタ
 33 A, 33 B フォトカプラ
 34 A, 34 B 発光ダイオード
 35 A, 34 B フォトトランジスタ
 36 A, 36 B フォトカプラ
 37 A, 37 B 発光ダイオード
 38 A, 38 B フォトトランジスタ
 39 A, 39 B 抵抗
 40 ダイオード40
 41 抵抗41
 42 A, 42 B 出力信号駆動回路
 43 A, 43 B 故障検出回路
 44 A, 44 B チェック信号発生回路
 45 A, 45 B 接点リードバック回路
 46 A, 46 B ダイオード
 47 制御処理手段
 48 交番信号発生手段

49 カウンタ
 50 走行フラグ
 51 カウンタ
 61 第1の制御処理端末装置
 62 第2の制御処理端末装置
 63~66 入出力処理端末装置
 67~70 現場機器
 71 A, 71 B, 71 C A系、B系及びC系マイクロ
 プロセッサ・コントローラ
 72 A, 72 B, 72 C マイクロプロセッサ・ユニッ
 ト
 73 A, 73 B, 73 C メモリ部
 74 A, 74 B, 74 C LAN制御部
 75 A, 75 B, 75 C I/Oバス・インタフェース
 76 A, 76 B, 76 C I/Oバス・インタフェース
 77 A, 77 B, 77 C 入力ユニット
 78 A, 78 B, 78 C 出力ユニット
 79 A, 79 B, 79 C ヘルシー回路
 80~82 共有メモリ
 83 現場機器入力信号モジュール
 84 現場機器出力信号モジュール
 85 A1, 85 A2 出力回路
 86 A1, 86 A2 トランス
 87 A1, 87 A2 ダイオード
 88 A1, 88 A2 リレー
 89 A1, 89 A2 ヘルシーリレー接点
 90 オンタイマリレー
 91 A系電源リレー
 92~97 接点
 98 主接点
 101 A, 101 B マイクロプロセッサ・ユニット
 102 A, 102 B メモリ
 103 クロック回路
 104 A, 104 B バス104
 105 バス照合・交番信号出力回路
 106 照合異常検出回路

【図8】

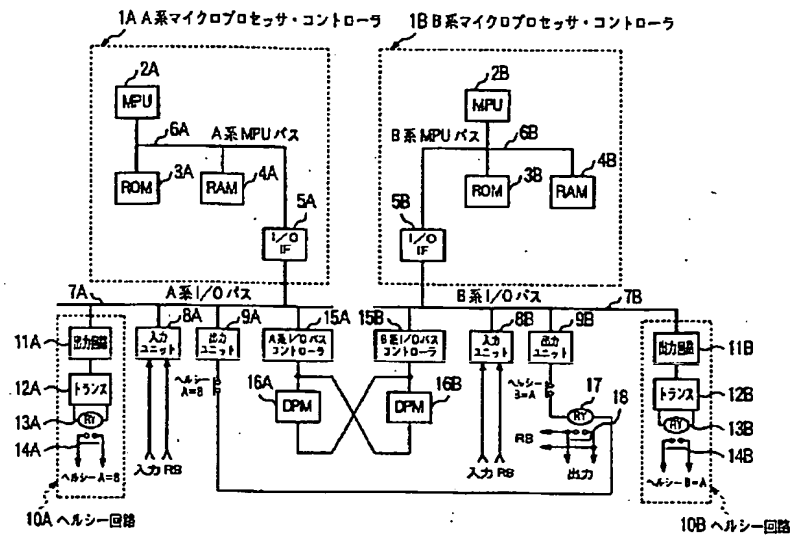


【図15】

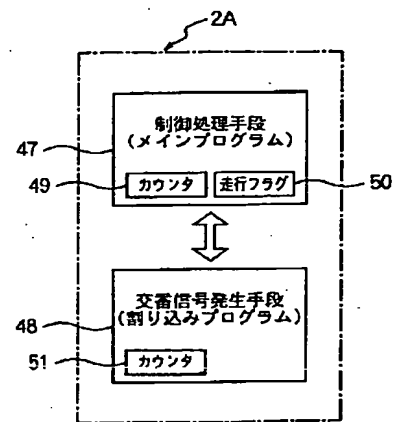
	A系		B系		C系		結果
	ヘルシー A=B	ヘルシー A=C	ヘルシー B=C	ヘルシー B=A	ヘルシー C=B	ヘルシー C=A	
1	0	0	1	0	1	0	多数決でA系のみを電源西
2	0	X ₂	X ₂	0	X ₁	X ₁	A系を電源断、B系も電源断
3	X ₂	0	X ₁	X ₁	X ₂	0	A系を電源断、C系も電源断

(18)

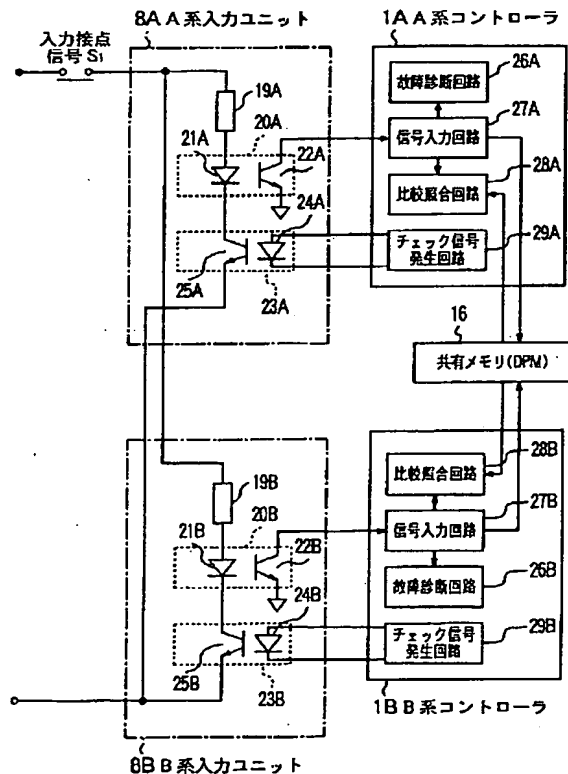
【図 1】



【図 9】



【図 2】

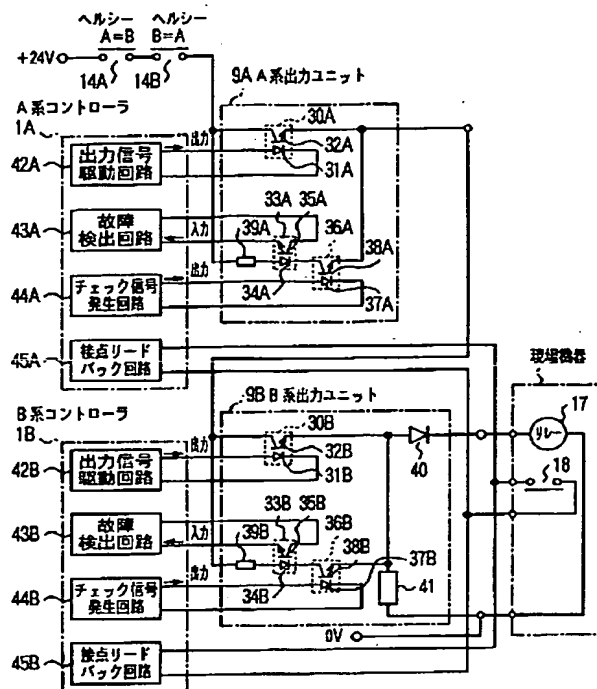


【図 3】

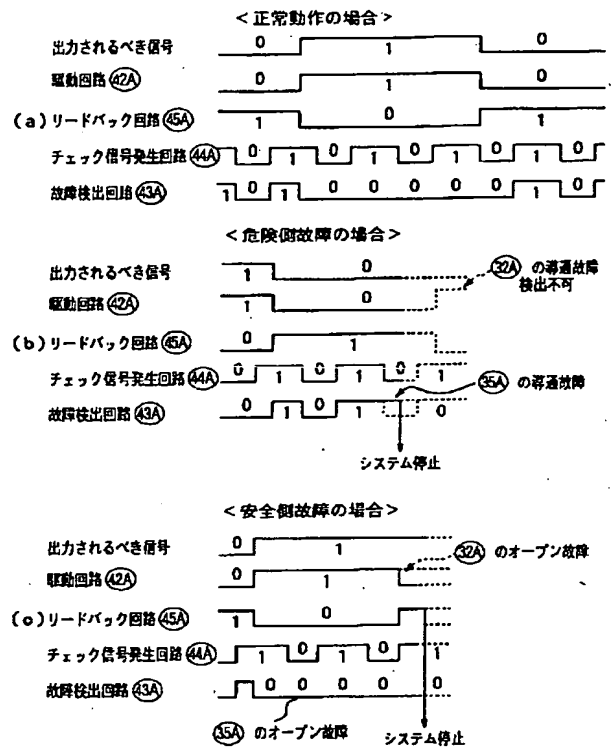
項目	入力接点	チェック信号	信号入力回路 ②の状態	実際の状態	コントローラ の判断
1	"0" = 開	0	0 (正常)	正常	正常
2	"0" = 開	1	0 (正常)	正常	正常
3	"0" = 開	0	0 (故障)	潜在故障	正常
4	"0" = 開	1	0 (故障)	潜在故障	正常
5	"0" = 開	0	1 (故障)	危険側故障	故障と判断
6	"0" = 開	1	1 (故障)	危険側故障	他系("0")との 照合で故障を検知
7	"0" = 開	0 (②の オン故障)	0 (正常)	潜在故障	正常
8	"0" = 開	1 (②の オフ故障)	0 (正常)	潜在故障	正常
9	"0" = 開	0 (②の オフ故障)	0 (正常)	潜在故障	正常
10	"0" = 開	1 (②の オフ故障)	0 (正常)	潜在故障	正常
11	"1" = 閉	0	0 (故障)	故障	他系("1")との 照合で故障を検知
12	"1" = 閉	1	0 (故障)	故障	他系("1")との 照合で故障を検知
13	"1" = 閉	0	0 (正常)	正常	正常
14	"1" = 閉	1	1 (正常)	正常	正常
15	"1" = 閉	0	1 (故障)	故障	故障と判断
16	"1" = 閉	1	1 (故障)	潜在故障	正常
17	"1" = 閉	0 (②が オン故障)	1 (正常)	故障	チェック中オフに ならず故障と判断
18	"1" = 閉	1 (②が オフ故障)	1 (正常)	潜在故障	正常
19	"1" = 閉	0 (②が オフ故障)	0 (正常)	故障	他系("1")との 照合で故障を検知
20	"1" = 閉	1 (②が オフ故障)	0 (正常)	故障	他系("1")との 照合で故障を検知

(19)

【図4】



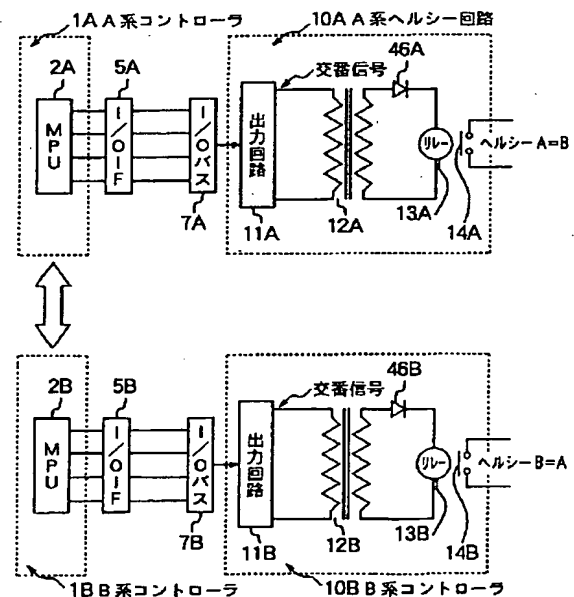
【図5】



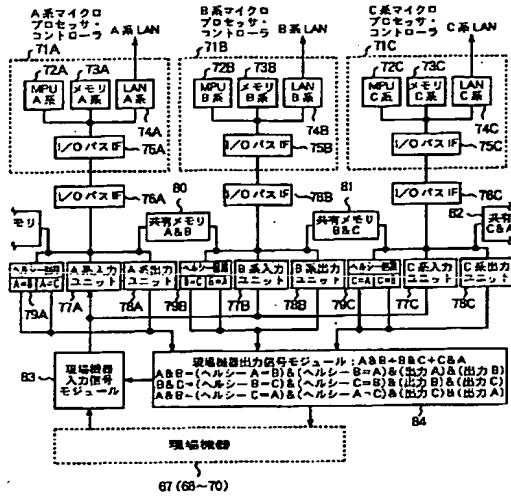
【図6】

項目	出力されるべき信号	リレーの動作	(42A) 駆動回路	(45A) R/B回路	(44A) チェック信号	(43A) 故障検出	コントローラの動作	実際の状態
1	0	無励磁	0: 正常 (42A) オフ	1: 正常 (45A) の故障 (45A) の故障	1: 正常	1: 正常	正常	正常
2	0	無励磁	0: 正常	0: 故障	0: チェック中	0: 正常	正常	正常
3	0	無励磁	0: 正常	0: 故障	1: 正常	1: 正常	出力故障 異常エラー	R/B回路 (45A) が異常
4	0	無励磁	0: 正常	1: 正常	0: チェック中	0: 正常	正常	(43A) が正常に故障、又は (45A) がオープン
5	0	無励磁	0: 正常	1: 正常	1: 正常	1: 正常	正常	(43A) が正常に故障、又は (45A) がオープン
6	0	無励磁	0: 正常	1: 正常	0: チェック中	0: 正常	正常	(43A) が正常に故障、又は (45A) がオープン
7	0	無励磁	0: 正常	1: 正常	1: 正常	1: 正常	正常	(43A) が正常に故障、又は (45A) がオープン
8	0	無励磁	0: 正常	1: 正常	0: チェック中	1: 故障	正常	(43A) が正常に故障、又は (45A) がオープン
9	0	無励磁	1: 故障 (42A) オフ	1: 正常	1: 正常	0: 正常	正常	(42A) が故障
10	0	無励磁	1: 故障 (42A) オフ	1: 正常	0: チェック中	0: 正常	正常	(42A) が故障
11	0	無励磁	1: 故障 (42A) オフ	1: 正常	1: 正常	1: 故障	正常	(42A) の故障は検出不可、(45A) の故障とみなす(2重故障)
12	0	無励磁	1: 故障 (42A) オフ	1: 正常	0: チェック中	1: 故障	正常	(42A) の故障は検出不可、(45A) の故障とみなす(2重故障)
13	1	励磁	1: 正常 (42A) オフ	0: 正常 (45A) の故障 (45A) の故障	1: 正常	0: 正常	正常	正常動作中
14	1	励磁	0: 故障 (42A) オフ	1: 正常	0: チェック中	0: 正常	正常	正常動作中
15	1	励磁	0: 故障 (42A) オフ	1: 正常	1: 正常	1: 正常	正常	正常動作中
16	1	励磁	0: 故障 (42A) オフ	1: 正常	0: チェック中	0: 正常	正常	正常動作中
17	1	励磁	1: 正常 (42A) オフ	1: 正常	1: 正常	0: 正常	正常	正常動作中
18	1	励磁	1: 正常 (42A) オフ	1: 正常	0: チェック中	0: 正常	正常	正常動作中
19	1	励磁	1: 正常 (42A) オフ	1: 正常	1: 正常	0: 正常	正常	正常動作中
20	1	励磁	1: 正常 (42A) オフ	1: 正常	0: チェック中	0: 正常	正常	正常動作中
21	1	励磁	0: 故障 (42A) オフ	1: 正常	1: 正常	0: 正常	正常	正常動作中
22	1	励磁	0: 故障 (42A) オフ	1: 正常	0: チェック中	0: 正常	正常	正常動作中

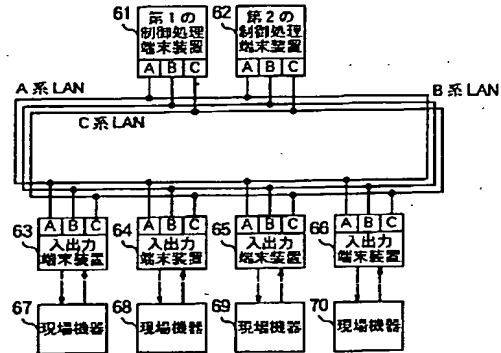
【図7】



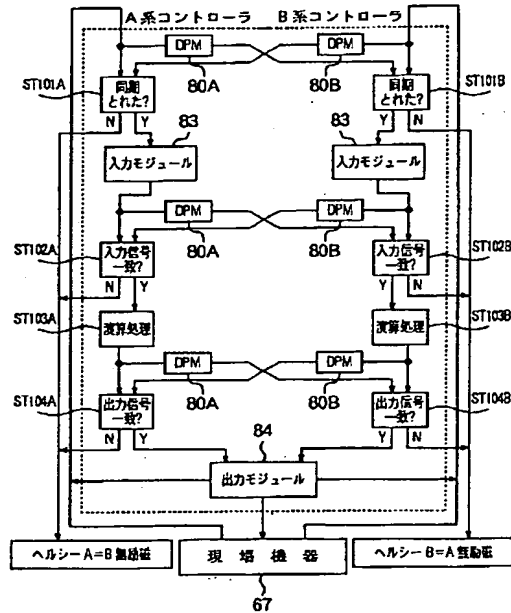
【図10】



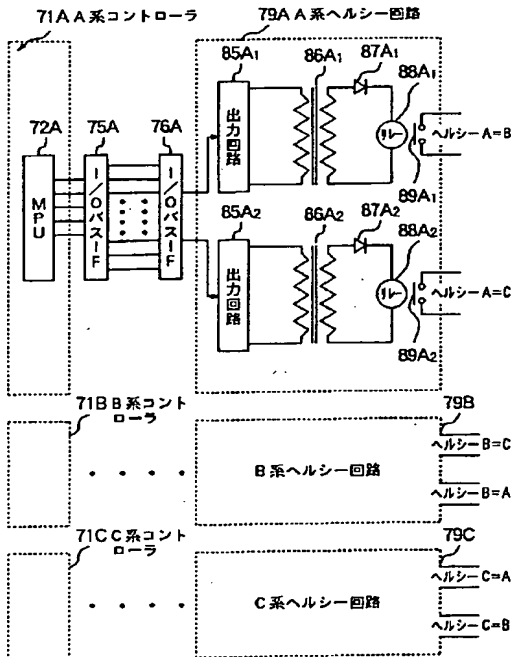
【図11】



【図13】

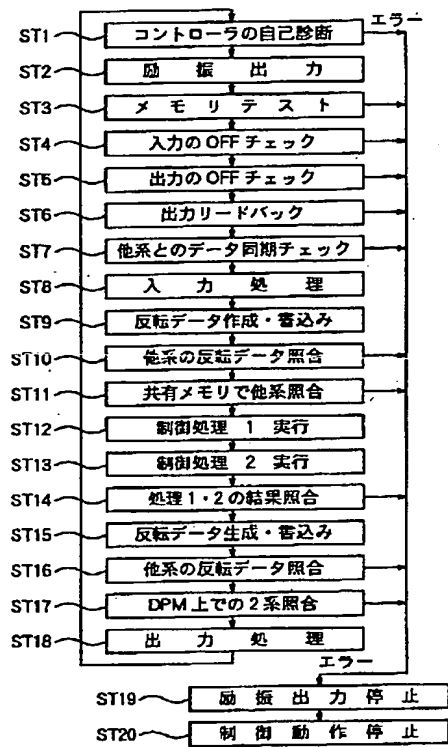


【図12】

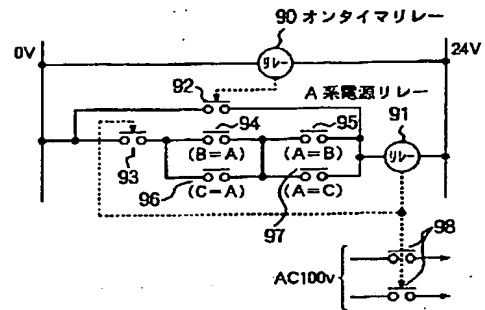


(21)

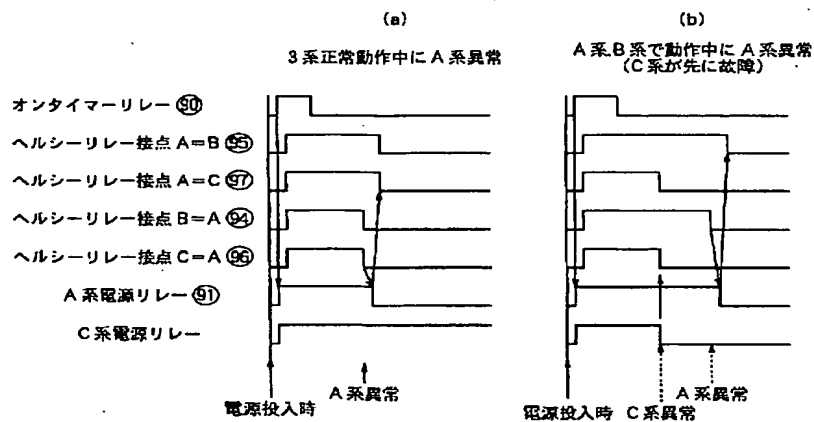
【図14】



【図16】

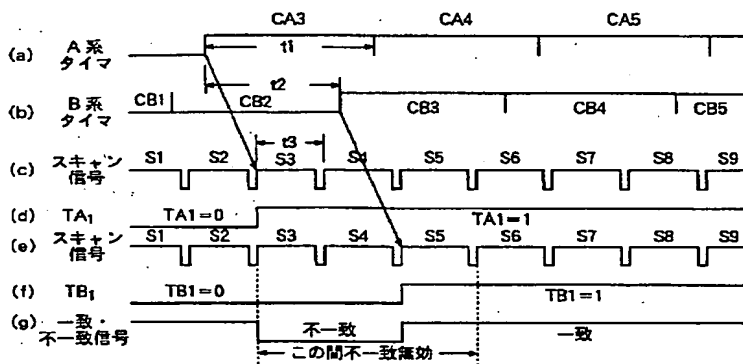


【図17】

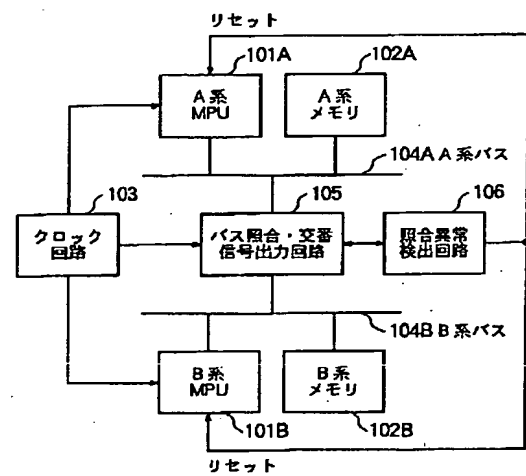


(22)

【図18】



【図19】



フロントページの続き

(72)発明者 目黒隆之
東京都渋谷区代々木二丁目2番2号 東日
本旅客鉄道株式会社内

(72)発明者 大谷祥之
東京都渋谷区代々木二丁目2番2号 東日
本旅客鉄道株式会社内

(72)発明者 磯野京介
東京都渋谷区代々木二丁目2番2号 東日
本旅客鉄道株式会社内

(72)発明者 永島暉造
東京都港区芝浦一丁目1番1号 株式会
社東芝本社事務所内

(72)発明者 安本高典
東京都港区芝浦一丁目1番1号 株式会
社東芝本社事務所内

Fターム(参考) 5H209 AA09 BB07 CC05 DD04 EE06
GG04 SS01 SS04 SS07 TT00

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.